FOURTH EDITION

WHAT WENT WRONG?

Case Histories of Process Plant Disasters

Trevor Kletz

FOURTH EDITION

WHAT WENT WRONG?

Case Histories of Process Plant Disasters

"Most of the incidents are very simple. No esoteric knowledge or detailed study was required to prevent them—only a knowledge of what had happened before, which this book provides."

—*Trevor Kletz*

Learn from the mistakes of others. This invaluable and respected book examines the causes and aftermaths of numerous plant disasters—almost every one of which could have been prevented. Case histories illustrate what went wrong and why it went wrong, and then guide you in how to circumvent similar tragedies.

Twenty percent of the information in this fourth edition is brand new, with fifteen new figures and photos to help you better recognize danger. Extensive references are a hallmark of this trusted volume.

New sections include:

Electrical isolation • Heat radiation
Cooling coils • Recent incidents • Vacuum relief valves • Accidents at sea • Fires
Problem sources • Emulsion breaking
Chimney effects • Interlock failure
Choosing materials.

Keep your plant running safely. No professional concerned with operating, maintaining, and designing process plants should be without this classic book.

FOURTH EDITION

WHAT WENT WRONG?

FOURTH EDITION

WHAT WENT WRONG?

Case Histories of Process Plant Disasters

Trevor Kletz

Gulf Professional Publishing
an imprint of Butterworth-Heinemann

To Denise,
Who waited while I
"scorned delights and lived laborious days"
but never saw the results.

WHAT WENT WRONG?

Case Histories of Process Plant Disasters

FOURTH EDITION

Copyright © 1999 by Elsevier. All rights reserved. Printed in the United States of America. This book, or parts thereof, may not be reproduced in any form without permission of the publisher.

Originally published by Gulf Publishing Company,
Houston, TX

10 9 8 7 6 5

The publisher offers special discounts on bulk orders of this book.
For information, please contact:
Manager of Special Sales
Elsevier Science
200 Wheeler Road
Burlington, MA 01803
Tel: 781-313-4700
Fax: 781-313-4802

For information on all Gulf publications available, contact our World Wide Web homepage at http://www.bh.com/gulf

Contents

Acknowledgments xi

Preface xiii

Units and Nomenclature xix

Chapter 1. **Preparation for Maintenance** 1

1.1 Isolation, 1
1.2 Identification, 11
1.3 Removal of hazards, 16
1.4 Procedures not followed, 24
1.5 Quality of maintenance, 32
1.6 A personal note, 44

Chapter 2. **Modifications** 48

2.1 Startup modifications, 48
2.2 Minor modifications, 49
2.3 Modifications made during maintenance, 55
2.4 Temporary modifications, 56
2.5 Sanctioned modifications, 58
2.6 Process modifications, 60
2.7 New tools, 63
2.8 Organizational changes, 64
2.9 Gradual changes, 66
2.10 Modification chains, 66
2.11 Modifications made to improve the environment, 69
2.12 Control of modifications, 74

Chapter 3. Accidents Caused by Human Error 78

3.1 Introduction, 78
3.2 Accidents caused by simple slips, 79
3.3 Accidents that could be prevented by better training, 90

Chapter 4. Labeling 98

4.1 Labeling of equipment, 98
4.2 Labeling of instruments, 101
4.3 Labeling of chemicals, 104
4.4 Labels not understood, 106

Chapter 5. Storage Tanks 108

5.1 Overfilling, 108
5.2 Overpressuring, 110
5.3 Sucking in, 114
5.4 Explosions, 117
5.5 Floating-roof tanks, 125
5.6 Miscellaneous incidents, 129
5.7 FRP tanks, 133

Chapter 6. Stacks 136

6.1 Stack explosions, 136
6.2 Blocked stacks, 140
6.3 Heat radiation, 142

Chapter 7. Leaks 144

7.1 Some common sources of leaks, 145
7.2 Control of leaks, 154
7.3 Leaks onto water, wet ground, or insulation, 159
7.4 Detection of leaks, 160
7.5 Fugitive emissions, 162

Chapter 8. Liquefied Flammable Gases 165

8.1 Major leaks, 166
8.2 Minor leaks, 174
8.3 Other leaks, 175

Chapter 9. Pipe and Vessel Failures 179

9.1 Pipe failures, 179
9.2 Pressure vessel failures, 195

Chapter 10. Other Equipment 205

10.1 Centrifuges, 205
10.2 Pumps, 206
10.3 Air coolers, 208
10.4 Relief valves, 209
10.5 Heat exchangers, 218
10.6 Cooling towers, 221
10.7 Furnaces, 221

Chapter 11. Entry to Vessels 229

11.1 Vessels not freed from hazardous material, 229
11.2 Hazardous materials introduced, 231
11.3 Vessels not isolated from sources of danger, 233
11.4 Unauthorized entry, 236
11.5 Entry into vessels with irrespirable atmospheres, 238
11.6 Rescue, 239
11.7 Analysis of vessel atmosphere, 241
11.8 What is a confined space?, 241
11.9 Every possible error, 242

Chapter 12. Hazards of Common Materials 244

12.1 Compressed air, 244
12.2 Water, 246
12.3 Nitrogen, 248
12.4 Heavy oils (including heat transfer oils), 255

Chapter 13. Tank Trucks and Cars 262

13.1 Overfilling, 262
13.2 Burst hoses, 263
13.3 Fires and explosions, 265
13.4 Liquefied flammable gases, 266
13.5 Compressed air, 266
13.6 Tipping up, 267
13.7 Emptying into or filling from the wrong place, 268
13.8 Contact with live power lines, 270

Chapter 14. Testing of Trips and Other Protective Systems 272

14.1 Testing should be thorough, 272
14.2 All protective equipment should be tested, 275
14.3 Testing can be overdone, 279
14.4 Protective systems should not reset themselves, 279
14.5 Trips should not be disarmed without authorization, 281
14.6 Instruments should measure directly what we need to know, 284
14.7 Trips are for emergencies, not for routine use, 285
14.8 Tests may find faults, 286
14.9 Some miscellaneous incidents, 286
14.10 Some accidents at sea, 287

Chapter 15. Static Electricity 290

15.1 Static electricity from flowing liquids, 291
15.2 Static electricity from gas and water jets, 293
15.3 Static electricity from powders and plastics, 294
15.4 Static electricity from clothing, 296

Chapter 16. Materials of Construction 299

16.1 Wrong material used, 299
16.2 Hydrogen produced by corrosion, 303
16.3 Other effects of corrosion, 305
16.4 Loss of protective coatings, 305
16.5 Some other incidents caused by corrosion, 306
16.6 Fires, 306
16.7 Choosing materials, 307

Chapter 17. Operating Methods 309

17.1 Trapped pressure, 309
17.2 Clearing choked lines, 311
17.3 Faulty valve positioning, 313
17.4 Responsibilities not defined, 314
17.5 Communication failures, 315
17.6 Work at open manholes, 318
17.7 One line, two duties, 318
17.8 Inadvertent isolation, 319
17.9 Incompatible storage, 319

17.10 Maintenance—is it really necessary?, 320
17.11 An interlock failure, 321
17.12 Emulsion breaking, 322
17.13 Chimney effects, 323

Chapter 18. Reverse Flow and Other Unforeseen Deviations 327

18.1 Reverse flow from a product receiver or blowdown line back into the plant, 327
18.2 Reverse flow into service mains, 329
18.3 Reverse flow through pumps, 331
18.4 Reverse flow from reactors, 331
18.5 Reverse flow from drains, 333
18.6 Other deviations, 334
18.7 A method for foreseeing deviations, 335
18.8 Some pitfalls in hazop, 337
18.9 Hazop of batch plants, 338
18.10 Hazop of tank trucks, 340

Chapter 19. I Didn't Know That 343

19.1 Ammonia can explode, 343
19.2 Hydraulic pressure tests can be hazardous, 345
19.3 Diesel engines can ignite leaks, 346
19.4 Carbon dioxide can ignite a flammable mixture, 348
19.5 Mists can explode, 348
19.6 The source of the problem lay elsewhere, 350

Chapter 20. Problems with Computer Control 353

20.1 Hardware and software faults, 353
20.2 Treating the computer as a black box, 354
20.3 Misjudging the way operators will respond, 359
20.4 Other problems, 360
20.5 Unauthorized interference, 362
20.6 New applications, 363
20.7 Conclusions, 365

Chapter 21. Inherently Safer Design 367

21.1 Bhopal, 368
21.2 Other examples of inherently safer design, 372
21.3 User-friendly design, 377

Chapter 22. Reactions—Planned and Unplanned 380

22.1 Lack of knowledge, 381
22.2 Poor mixing, 383
22.3 Contamination, 385
22.4 Reactions with auxiliary materials, 387
22.5 Poor training or procedures, 387
22.6 Use-by dates, 388

Appendix 1. Relative Frequencies of Incidents 392

Appendix 2. Final Thoughts 395

Appendix 3. Recommended Reading 397

Index 399

Acknowledgments

Thanks are due to the staffs of the companies where the incidents occurred for allowing me to describe their mistakes; to many colleagues, past and present, especially to Professor F. P. Lees for his ideas and advice; and to the UK Science and Engineering Research Council and the Leverhulme Trust for their financial support.

Preface

In 1968, after many years' experience in plant operations, I was appointed safety adviser to the heavy organic chemicals division (later the petrochemicals division) of Imperial Chemical Industries. My appointment followed a number of serious fires in the 1960s, and therefore I was mainly concerned with process hazards rather than those of a mechanical nature.

One of my tasks was to pass on to design and operating staff details of accidents that had occurred and the lessons that should be learned. This book contains a selection of the reports I collected from many different companies. Although most have been published before, they were scattered among many different publications, some with small circulations.

The purpose here is to show what has gone wrong in the past and to suggest how similar incidents might be prevented in the future. Unfortunately, the history of the process industries shows that many incidents are repeated after a lapse of a few years. People move on, and the lessons are forgotten. This book will help keep the memories alive.

The advice is given in good faith but without warranty. Readers should satisfy themselves that it applies to their circumstances. In fact, you may feel that some of my recommendations are not appropriate for your company. Fair enough, but if the incidents could occur in your company, and you do not wish to adopt my advice, then please do something else instead. But do not ignore the incidents.

To quote the advice of John Bunyan, written more than 300 years ago,

> What of my dross thou findest there, be bold
> To throw away, but yet preserve the gold.

What if my gold be wrapped up in ore?
None throws away the apple for the core:
But if thou shalt cast all away as vain . . .

You have been warned what will happen.

You may believe that the accidents could not happen at your plant because you have systems to prevent them. Many of the accidents I describe occurred on plants that had such systems, but the systems were not always followed. The accidents happened because of various management failures: failure to convince people that they should follow the systems, failure to detect previous violations (by audits, spot checks, or just keeping an open eye), or deliberately turning a blind eye to avoid conflict or to get a job done quickly. The first step down the road to many a serious accident occurred when someone turned a blind eye to a missing blind (see Chapter 1).

The incidents described could occur in many different types of plants and are therefore of widespread interest. Some of them illustrate the hazards involved in activities such as preparing equipment for maintenance and modifying plants. Others illustrate the hazards associated with widely used equipment, such as storage tanks and hoses, and with that universal component of all plants and processes: people. Other incidents illustrate the need for techniques, such as hazard and operability studies, and protective devices, such as emergency isolation valves.

You will notice that most of the incidents are very simple. No esoteric knowledge or detailed study was required to prevent them—only a knowledge of what had happened before, which this book provides.

Only a few incidents started with the sudden failure of a major component. Most started with a flaw in a minor component, an instrument that was out of order or not believed, a poor procedure, or a failure to follow procedures or good engineering practice. *For want of a nail, the battle was lost.*

Many of the incidents described could be discussed under more than one heading. Therefore, cross-references have been included.

If an incident that happened in your plant is described, you may notice that one or two details have been changed. Sometimes this has been done to make it harder for people to tell where the incident occurred. Sometimes this has been done to make a complicated story simpler but without affecting the essential message. Sometimes—and this is the most likely

reason—the incident did not happen in your plant at all. Another plant had a similar incident.

Many of the incidents did not actually result in death, serious injury, or serious damage—they were near-misses. But they could have had much more serious consequences. We should learn from these near-misses, as well as from incidents that had serious results.

Most of the incidents described occurred at so-called major hazard plants or storage installations—that is, those containing large quantities of flammable, explosive, or toxic chemicals. The lessons learned apply particularly to such plants. However, most of the incidents could have occurred at plants handling smaller quantities of materials or less hazardous materials, and the consequences, though less serious, would be serious enough. At a major-hazard plant, opening up a pump that is not isolated could cause (and has caused) a major fire or explosion. At other plants, this would cause a smaller fire or a release of corrosive chemicals—still enough to kill or injure the employee on the job. Even if the contents of the plant are harmless, there is still a waste of materials. The lessons to be learned therefore apply throughout the process industries.

For the second edition of this book, I added more incidents, extended the sections on Bhopal and Mexico City, and added chapters on some little-known but quite common hazards and on accidents in computer-controlled plants.

For the third edition, I added sections or chapters on heat exchangers, furnaces, inherently safer design, and runaway reactions, and extended many other chapters. Although I have read many accident reports since the first edition appeared, most have merely reinforced the messages of the book, and I added only those incidents that tell us something new.

For this fourth edition, I have added further incidents to every chapter.

This book is concerned with the immediate technical causes of accidents and the changes in design and procedures needed to prevent them from happening again. The underlying causes—management weaknesses such as failures to learn the lessons of the past, failures to audit, and superficial investigation of incidents—are discussed in some of my other books such as *Lessons from Disaster: How Organizations Have No Memory and Accidents Recur* (Institution of Chemical Engineers/Gulf Publishing Co., 1993) and *Learning from Accidents,* 2nd edition (Butterworth-Heinemann, 1994).

Most of the incidents described were the result of not following good engineering practice. Some violated the law, and many more would if they occurred today. In the United States, they would violate OSHA 1910.147 (1990) on The Control of Hazardous Energy (Lock Out/Tag Out) and the Process Safety Management (PSM) Law (OSHA 1910.119, in force since 1992), which applies to listed chemicals above a threshold quantity. The PSM Law requires companies to follow good engineering practice, codes, industry consensus standards, and even the company's own standards. OSHA could view failure to follow any of these as violations.

In the United Kingdom, the Health and Safety at Work Act (1974) and regulations made under it require "occupiers" to provide a safe plant and system of work and adequate instruction, training, and supervision. In the European community, occupiers of major hazard sites are required to produce a "safety case," which describes how hazards have been assessed and are kept under control. Many other countries have similar legislation, though standards of enforcement vary.

As a result of OSHA 1910.119 and similar legislation, there has been a growth of interest in process safety management systems and publications on them. This is welcome, but we must not forget their limitations. Some managers seem to think a good system is all that is needed to ensure safety. However, all a system can do is harness the knowledge and experience of people. If knowledge and experience have been downsized away, the system is an empty shell. Knowledge and experience without a system will achieve less than their full potential. Without knowledge and experience, a system will achieve nothing. We are not going to prevent downsizing, but we can ensure that the lessons of the past are not forgotten. The book tries to contribute to the achievement of that aim.

HOW TO USE THIS BOOK

1. Read it right through. As you do so, ask yourself if the incidents could occur in *your* plant, and, if so, *write down* what you intend to do to prevent them from occurring.
2. Use it as a deskside book on safety. Dip into it at odd moments or pick a subject for the staff meeting, the safety committee or bulletin, or the plant inspection.
3. Refer to it when you become interested in something new as the result of an incident, a change in responsibility, or a new problem in design. However, this book does not claim to comprehensively

review process safety and loss prevention. For that, refer to F. P. Lees' *Loss Prevention in the Process Industries,* 2nd edition (Butterworth-Heinemann, Oxford, UK, 1996, 3 volumes).

4. Use the incidents to train new staff, managers, foremen, and operators so they know what will happen if they do not follow recognized procedures and good operating practice.
5. If you are a teacher, use the incidents to tell your students why accidents occur and to illustrate scientific principles.

   Both in the training of plant staff and students, the material can be used as lecture material or, better, as discussion material (those present discuss and agree among themselves what they think should be done to prevent similar incidents from happening again). The use of case histories in this way is discussed in my book, *Lessons From Disaster: How Organizations Have No Memory and Accidents Recur* (Institution of Chemical Engineers/Gulf Publishing Co., 1993, Chapter 10).
6. If you want to be nasty, send a copy of the book, open at the appropriate page, to people who have allowed one of the accidents described to happen again. They may read the book and avoid further unnecessary accidents.

A high price has been paid for the information in this book: many persons killed and billions of dollars worth of equipment destroyed. You get this information for the price of the book. It will be the best bargain you have ever received if you use the information to prevent similar incidents at your plant.

Trevor Kletz

This book will make a traveller of thee,
If by its counsel thou wilt ruled be.
It will direct thee to a safer land
If thou wilt its directions understand.

—Adapted from R. Vaughan Williams'
libretto for *The Pilgrim's Progress*

PRINCIPAL ADDITIONS TO FOURTH EDITION

1.1.7
1.2.1(g)–(h)
1.2.3(e)
1.3.1(g)
1.3.3(c)
1.4.5(d)–(e)
1.4.6
1.5.1(b)
1.5.7–1.6
2.2(d)–(e)
2.3 (end)
2.6(h)–(j)
2.11.1 (end)
3.1 (part)
3.2.1 (part)
3.2.7(b)
3.3.2(c)–(d)
4.1(g)–(j)
4.2(g)
4.3.1 (part)
4.3.2 (part)
5.2.1 (end)
5.4.2(d)–(f)
5.7(h)
6.1(e)–(f)
6.3
7.1.2 (part)
7.1.3 (part)
7.1.4 (part)
7.1.6(c)–(d)
7.1.7
7.2.1 (part)
7.4 (part)
8.1.6
9.1.2(a) (part)
9.2.1(g)–(i)
9.2.2(e)
9.2.3(c)
10.4.5 (end)
10.4.6 (end)
10.4.7(b)–(c)
11.1(g)
11.4(d)–(e)
11.6(c)
11.9
12.4.1 (part)
13.7 (part)
14.1(f)–(h)
14.2.5(c)
14.5(c)–(g)
14.10
15.3 (part)
16.1(a),(j),(n) (parts)
16.6–7
17.1 (part)
17.11–13
18.8–9
19.1 (part)
19.5 (part)
19.6
20.1 (part)
20.4.3–4
20.5 (part)
20.6
21.2.1 (part)
21.2.2 (part)
21.2.6
22.2.1(d)–(e)
22.2.2(d)–(e)
Appendix 1
Appendix 2

Units and Nomenclature

I have used units likely to be most familiar to the majority of my readers. Although I welcome the increasing use of SI units, many people still use imperial units—they are more familiar with a 1-in. pipe that a 25-mm pipe.

Short lengths are therefore quoted in inches but longer lengths in meters.

1 in. = 25.4 mm

1 m = 3.28 ft or 1.09 yd

Volumes are quoted in cubic meters (m^3), as this unit is widely used and *gallons* is ambiguous.

$1\ m^3$ = 264 U.S. gallons

= 220 imperial gallons

= $35.3\ ft^3$

A tank 30 ft tall by 40 ft diameter has a volume of $1{,}068\ m^3$ (280,000 U.S. gallons); a tank 15 ft tall by 20 ft diameter has a volume of $133\ m^3$ (35,250 U.S. gallons).

Masses are quoted in kilograms (kg) or tons.

1 kg = 2.20 lb

1,000 kg = 1 metric tonne = 1.10 short (U.S.) tons

= 0.98 long (UK) ton

Temperatures are quoted in °C.

Pressures are quoted in pounds force per square inch (psi) and also in bars. As it is not usual to refer to bar gauge, I have, for example, referred to "a gauge pressure of 90 psi (6 bar)," rather than "a pressure of 90 psig."

1 bar = 14.50 psi

= 1 atmosphere (atm)

= 1 kg/cm^2

= 100 kilopascals (kPa)

Very small gauge pressures are quoted in inches water gauge, as this gives a picture.

1 in. water gauge = 0.036 psi

= 2.5 x 10^{-3} bar

= 0.2 kPa

A NOTE ABOUT NOMENCLATURE

Different words are used, in different countries, to describe the same job or piece of equipment. Some of the principal differences between the United States and the United Kingdom are listed here. Within each country, however, there are differences between companies.

Management Terms

Job	U.S.	UK
Operator of plant	Operator	Process worker
Operator in charge of others	Lead operator	Chargehand or Assistant foreman or Junior supervisor
Highest level normally reached by promotion from operator	Foreman	Foreman or Supervisor
First level of professional management (usually in charge of a single unit)	Supervisor	Plant manager
Second level of professional management	Superintendent	Section manager
Senior manager in charge of site containing many units	Plant manager	Works manager
Plant personnel	Craftsman or mechanic	Fitter, electrician, etc.

The different meanings of the terms *supervisor* and *plant manager* in the U.S. and UK should be noted.

In this book I have used the term *foreman* as it is understood in both countries, though its use in the UK is becoming outdated. *Manager* is used to describe any professionally qualified person in charge of a unit or group of units. That is, it includes people who, in many U.S. companies, would be described as supervisors or superintendents.

Certain items of plant equipment have different names in the two countries. Some common examples are:

Chemical Engineering Terms

U.S.	UK
Accumulator	Reflux drum
Agitator	Mixer or stirrer
Air masks	Breathing apparatus (BA)
Blind	Slip-plate
Carrier	Refrigeration plant
Cascading effects	Knock-on (or domino effects)
Check valve	Nonreturn valve
Clogged (of filter)	Blinded
Consensus standard	Code of practice
Conservation vent	Pressure/vacuum valve
Dike, berm	Bund
Discharge valve	Delivery valve
Division (in electrical area classification)	Zone
Downspout	Downcomer
Expansion joint	Bellows
Explosion proof	Flameproof
Faucet	Tap
Fiberglass-reinforced plastic (FRP)	Glass-reinforced plastic (GRP)
Figure-8 plate	Spectacle plate
Flame arrestor	Flame trap
Flashlight	Torch
Fractionation	Distillation
Gasoline	Petrol
Gauging (of tanks)	Dipping
Generator	Dynamo or alternator
Ground	Earth
Horizontal cylindrical tank	Bullet
Hydro (Canada)	Electricity
Install	Fit
Insulation	Lagging
Interlock*	Trip*
Inventory	Stock
Lift-truck	Forklift truck
Loading rack	Gantry

U.S.	UK
Manway	Manhole
Mill water	Cooling water
Nozzle	Branch
OSHA (Occupational Safety and Health Administration)	Health and Safety Executive
Pedestal, pier	Plinth
Pipe diameter (internal)	Pipe bore
Pipe rack	Pipebridge
Plugged	Choked
Rent	Hire
Rupture disc or frangible	Bursting disc
Scrutinize	Vet
Seized (of a valve)	Stuck shut
Shutdown	Permanent shutdown
Sieve tray	Perforated plate
Siphon tube	Dip tube
Spade	Slip-plate
Sparger or sparge pump	Spray nozzle
Spigot	Tap
Spool piece	Bobbin piece
Stack	Chimney
Stator	Armature
Tank car	Rail tanker or rail tank wagon
Tank truck	Road tanker or road tank wagon
Torch	Cutting or welding torch
Tower	Column
Tow motor	Forklift truck
Tray	Plate
Turnaround	Shutdown
Utility hole	Manhole
Valve cheater	Wheel dog
Water seal	Lute
Wrench	Spanner
C-wrench	Adjustable spanner
Written note	Chit
$M	Thousand dollars
$MM	$M or million dollars
STP	60°F, 1 atmosphere
32°F, 1 atmosphere	STP
NTP	32°F, 1 atmosphere

**In the UK,* interlock *is used to describe a device that prevents someone opening one valve while another is open (or closed).* Trip *describes an automatic device that closes (or opens) a valve when a temperature, pressure, flow, etc., reaches a preset value.*

Fire-Fighting Terms

U.S.	UK
Dry chemical	Dry powder
Dry powder	Dry powder for metal fires
Egress	Escape
Evolutions	Drills
Excelsior (for fire tests)	Wood wool
Fire classification:	
Class A: Solids	Class A: Solids
Class B: Liquids and gases	Class B: Liquids
Class C: Electrical	Class C: Gases
Class D: Metals	Class D: Metals
Fire stream	Jet
Nozzle	Branchpipe
Open butt	Hose without branchpipe
Rate density	Application rate
Siamese connection	Collecting breeching
Sprinkler systems:	
Branch pipe	Range pipe
Cross main	Distribution pipe
Feed main	Main distribution pipe
Standpipe	Dry riser
Tip	Nozzle
Wye connection	Dividing breeching

Chapter 1

Preparation for Maintenance

> Mr. Randall (factory inspector) said he was surprised at the system of work, as he knew the company's safety documents were very impressive. Unfortunately they were not acted upon.
>
> —*Health and Safety at Work*, April 1996

The following pages describe accidents that occurred because equipment was not adequately prepared for maintenance. Sometimes the equipment was not isolated from hazardous materials; sometimes it was not identified correctly, and so the wrong equipment was opened up; sometimes hazardous materials were not removed [1, 2].*

Entry to vessels is discussed in Chapter 11.

1.1 ISOLATION

1.1.1 Failure to Isolate

A pump was being dismantled for repair. When the cover was removed, hot oil, above its auto-ignition temperature, came out and caught fire. Three men were killed, and the plant was destroyed. Examination of the wreckage after the fire showed that the pump suction valve was open and the drain valve shut [3].

*End-of-chapter references are indicated by a number inside brackets.

The pump had been awaiting repair for several days when a permit-to-work was issued at 8 a.m. on the day of the fire. The foreman who issued the permit should have checked ahead of time that the pump suction and delivery valves were shut and the drain valve open. He claimed that he did so. Either his recollection was incorrect or, after he inspected the valves and before work started, someone closed the drain valve and opened the suction valve. When the valves were closed, there was no indication—on them—of *why* they were closed. An operator might have opened the suction valve and shut the drain valve so that the pump could be put on line quickly if required.

A complicating factor was that the maintenance team originally intended to work only on the pump bearings. When team members found that they had to open up the pump, they told the process team, but no further checks of the isolations were carried out.

It was not customary in the company concerned to isolate equipment under repair by slip-plates, only by closed valves. But after the fire, the company introduced the following rules:

(a) Equipment under repair must be isolated by slip-plates (blinds or spades) or physical disconnection unless the job to be done will be so quick that fitting slip-plates (or disconnecting pipework) would take as long as the main job and be as hazardous. If hot work is to be carried out or a vessel is to be entered, then slip-plating or physical disconnection must always take place.

(b) Valves isolating equipment under maintenance, including valves that have to be closed while slip-plates are fitted (or pipework disconnected), must be locked shut with a padlock and chain or similar device. A notice fixed to the valve is not sufficient.

(c) For fluids at gauge pressures above 600 psi (40 bar) or at a temperature near or above the auto-ignition point, double block and bleed valves should be installed—not for use as main isolations but so that slip-plates can be inserted safely (Figure 1-1).

(d) If there is any change in the work to be done, the permit-to-work must be withdrawn and a new one issued.

A similar but more serious incident occurred in a polyethylene plant in 1989. A take-off branch was dismantled to clear a choke. The 8-in. valve isolating it from the reactor loop (the Demco valve in Figure 1-2) was open, and hot ethylene under pressure came out and exploded, killing 23

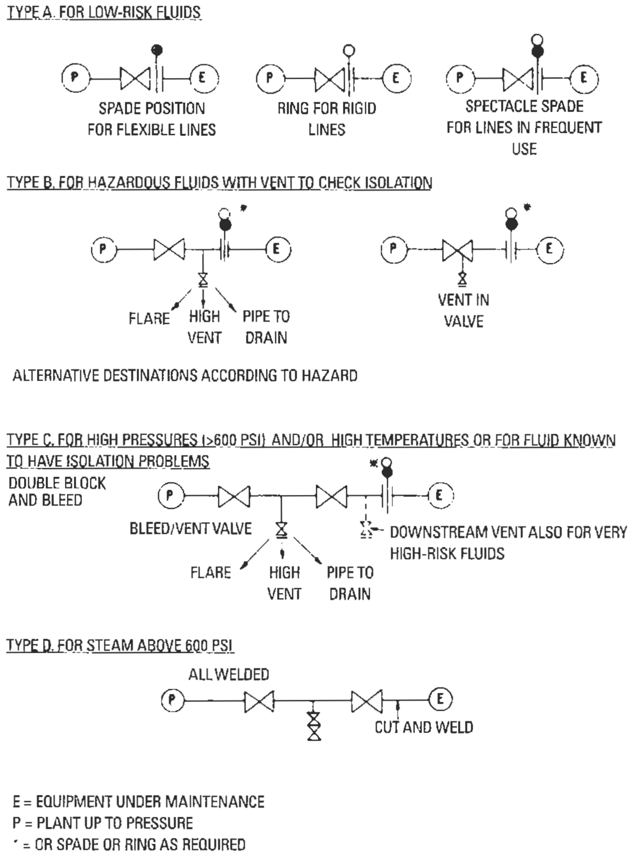


Figure 1-1. Summary of isolation methods.

people, injuring more than 130, and causing extensive damage. Debris was thrown six miles, and the subsequent fire caused two liquefied petroleum gas tanks to burst.

The valve was operated by compressed air, and the two air hoses, one to open the valve and one to close it, were connected up the wrong way around. The two connectors should have been different in size or design so that this could not occur. In addition, they were not disconnected, and a lockout device on the valve—a mechanical stop—had been removed. It is also bad practice to carry out work on equipment isolated from hot flammable gas under pressure by a single isolation valve. The take-off branch should have been slip-plated, and double block and bleed valves should have been provided so the slip-plate could be inserted safely (Figure 1-1), [16, 17].

There was another similarity to the first incident. In this case the equipment also had been prepared for repair and then had to wait for a couple of days until the maintenance team was able to work on it. During this period, the air lines were reconnected, the lockout removed, and the isolation valve opened.

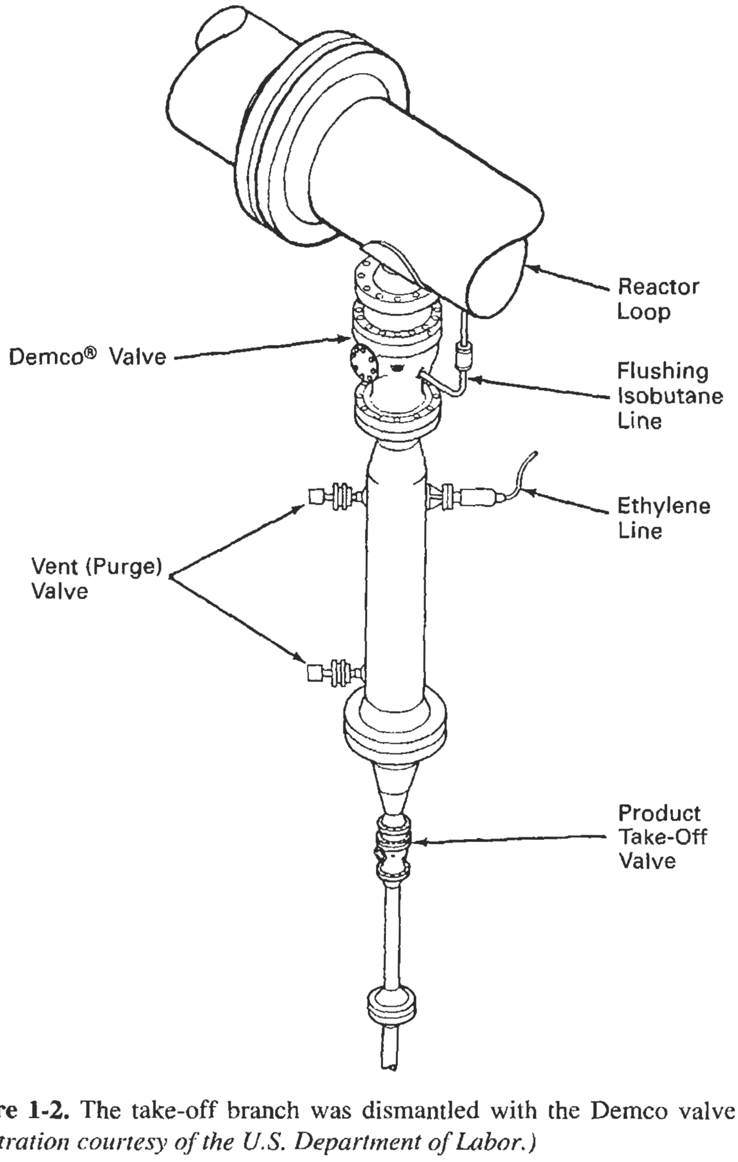


Figure 1-2. The take-off branch was dismantled with the Demco valve open. *(Illustration courtesy of the U.S. Department of Labor.)*

In both incidents, the procedures were poor and were not followed. It is unlikely that the accidents occurred the first time this happened. If the managers had kept their eyes open, they might have seen that the procedures were not being followed.

The 1988 explosion and fire on the Piper Alpha oil platform in the North sea, which killed 163 people, was also caused by poor isolation. A pump relief valve was removed for overhaul and the open end blanked. Another shift, not knowing that the relief valve was missing, started up the pump. The blank was probably not tight, and light oil leaked past it and exploded in the confined processing area. The official report [18] concluded ". . . that the operating staff had no commitment to working to the written procedure; and that the procedure was knowingly and flagrantly disregarded." The loss of life was greater on Piper Alpha than on the other two incidents because oil platforms are very congested and escape is difficult.

Section 18.1 describes other similar incidents.

1.1.2 Isolations Removed too Soon

An ethylene compressor was shut down for maintenance and correctly isolated by slip-plates. When repairs were complete, the slip-plates were removed before the machine was tried out. During the tryout, some ethylene leaked through the closed isolation valves into the machine. The ethylene/air mixture was ignited, either by a hot spot in the machine or by copper acetylide on the copper valve gaskets. The compressor was severely damaged.

Isolations should not be removed until maintenance is complete. It is good practice to issue three work permits—one for inserting slip-plates (or disconnecting pipework), one for the main job, and one for removing slip-plates (or restoring disconnections).

A similar incident occurred on a solids drier. Before maintenance started, the end cover was removed, and the inlet line was disconnected. When maintenance was complete, the end cover was replaced, and at the same time the inlet pipe was reconnected. The final job was to cut off the guide pins on the cover with a cutting disc. The atmosphere outside (but not inside) the drier was tested, and no flammable gas was detected. While cutting was in progress, an explosion occurred in the drier. Some solvent had leaked into the inlet pipe and then drained into the drier [19].

The inlet line should not have been reconnected before the guide pins were cut off.

1.1.3 Inadequate Isolation

A reactor was prepared for maintenance and washed out. No welding needed to be done, and no entry was required, so it was decided not to slip-plate off the reactor but to rely on valve isolations. Some flammable vapor leaked through the closed valves into the reactor and was ignited by a high-speed abrasive wheel, which was being used to cut through one of the pipelines attached to the vessel. The reactor head was blown off and killed two men. It was estimated that 7 kg of hydrocarbon vapor could have caused the explosion.

After the accident, demonstration cuts were made in the workshop. It was found that as the abrasive wheel broke through the pipe wall, a small flame occurred, and the pipe itself glowed dull red.

The explosion could have been prevented by isolating the reactor by slip-plates or physical disconnection. This incident and the others described show that valves are not good enough.

1.1.4 Isolation of Service Lines

A mechanic was affected by fumes while working on a steam drum. One of the steam lines from the drum was used for stripping a process column operating at a gauge pressure of 30 psi (2 bar). A valve on the line to the column was closed, but the line was not slip-plated. When the steam pressure was blown off, vapors from the column came back through the leaking valve into the steam lines (Figure 1-3).

The company concerned normally used slip-plates to isolate equipment under repair. On this occasion, no slip-plate was fitted because it was "only" a steam line. However, steam and other service lines in plant areas are easily contaminated by process materials, especially when there is a direct connection to process equipment. In these cases, the equipment under repair should be positively isolated by slip-plating or disconnection before maintenance.

When a plant was taken out of use, the cooling water lines were left full of water. Dismantling started nearly 20 years later. When a mechanic cut a cooling water line open with a torch, there was a small fire. Bacteria had degraded impurities in the water, forming hydrogen and methane [20].

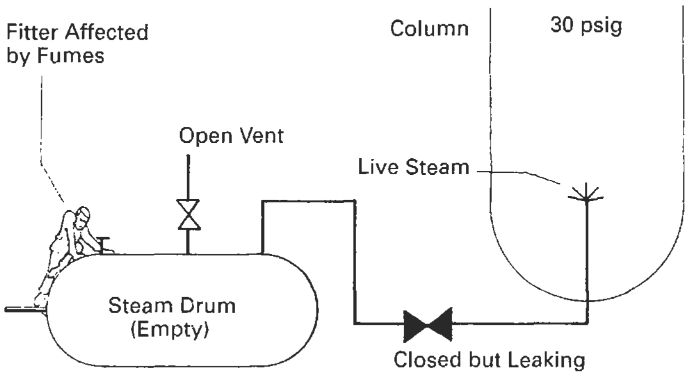


Figure 1-3. Contamination of a steam drum by process materials.

Plants should be emptied before they are mothballed or left for dismantling. Apart from the hazard just described, water can freeze and rupture lines (see Section 9.1.1).

Many years ago, river water was used for the water layer in a large kerosene storage tank. Bacterial decomposition of impurities formed methane, which exploded. As so often happens, the source of ignition was never found [21].

1.1.5 Isolations Not Removed

While a plant was on line, an operator noticed a slip-plate on a tank vent. The slip-plate had been fitted to isolate the tank from the blowdown system while the tank was under maintenance. When the maintenance was complete, the slip-plate was overlooked. Fortunately, the tank, an old one, was stronger than it needed to be for the duty, or it would have burst.

If a vessel has to be isolated from the vent or blowdown line, do not slip-plate it off, but whenever possible, disconnect it and leave the vessel vented to atmosphere (as shown in Figure 1-4).

If the vent line forms part of a blowdown system, it will have to be blanked to prevent air being sucked in. Make sure the blank is put on the flare side of the disconnection, not on the tank side (Figure 1-4). Note that if the tank is to be entered, the joint nearest the tank should be broken.

If a vent line has to be slip-plated because the line is too rigid to be moved, then the vents should be slip-plated last and de-slip-plated first. If all slip-plates inserted are listed on a register, they are less likely to be overlooked.

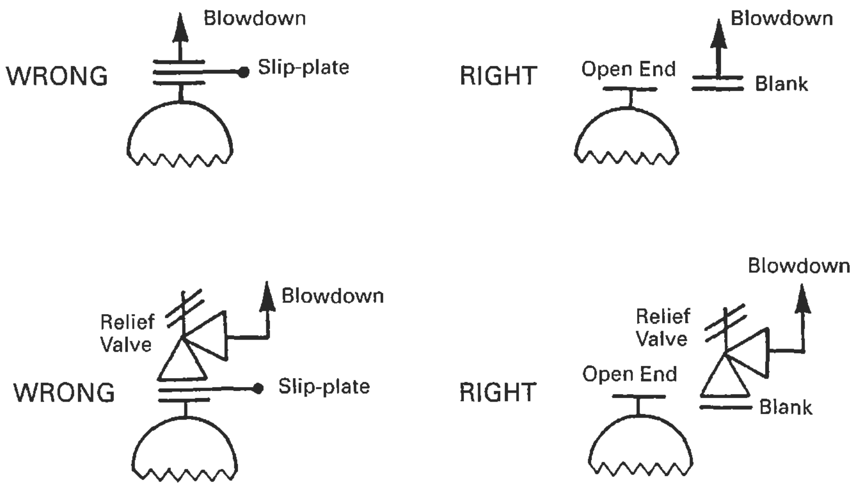


Figure 1-4. The right and wrong ways to isolate a vent line.

1.1.6 Some Miscellaneous Incidents Involving Isolation for Maintenance

(a) A slip-plate that had been in position for many months, perhaps years, was relied on to isolate equipment. It had corroded right through (Figure 1-5). Slip-plates in position for a long time should be removed and inspected before being used as maintenance isolations. (Such slip-plates should be registered for inspection every few years.)

(b) A slip-plate with a short tag was overlooked and left in position when maintenance was complete. Tags should be at least 130 mm long on lines up to and including 6-in. diameter and at least 150 mm long on larger lines. Figure-8 plates are better than slip-plates, as their position can be seen at a glance; Figure-8 plates should be used on lines that have to be slip-plated regularly. Although the initial cost is higher, they are always available on the job, while slip-plates tend to disappear and have to be replaced.

(c) On several occasions small bore branches have been covered by insulation, overlooked, and not isolated.

(d) On several occasions thin slip-plates have been used and have become bowed; they are then difficult to remove. Figure 1-6 shows a thin slip-plate that has been subjected to a gauge pressure of 470 psi (32 bar).

Figure 1-5. A slip-plate left in position for many months had corroded right through.

Figure 1-6. A slip-plate bowed by a gauge pressure of 470 psi (32 bar).

Slip-plates should normally be designed to withstand the same pressure as the piping. However, in some older plants that have not been designed to take full-thickness slip-plates, it may be impossible to insert them. A compromise will be necessary.

(e) A butane pump was isolated for repair by valves only. When it was opened up, the pump and adjoining lines were found to be full of hydrate, a compound of water and butane that stays solid at a higher temperature than ice. A steam hose was used to clear the choke. Soon afterward there was a leak of butane, which was ignited by a furnace 40 m away and exploded. The suction valve was also blocked by ice and was one turn open [22].

If you are not convinced that all isolation valves should be backed up by slip-plates before maintenance takes place, at least back up valves on lines containing materials that might turn solid and then melt.

1.1.7 Electrical Isolation

When an electrical supply has been isolated, it is normal practice to check that the right switches have been locked or fuses removed by trying to start the equipment that has been isolated. However, this system is not foolproof, as shown by the following incidents.

In one case the wrong circuit was isolated, but the circuit that should have been isolated was dead because the power supply had failed. It was restored while work was being carried out. In another case the circuit that should have been isolated fed outside lighting. The circuit was dead because it was controlled by a photo-eye control [41].

On several occasions maintenance teams have not realized that by isolating a circuit they have also isolated equipment that was still needed. In one case they isolated heat tracing tape and, without realizing it, also isolated a ventilation fan. The wiring was not in accordance with the drawings [42]. In another case maintenance team members isolated a power supply without realizing that they were also isolating the power to nitrogen blanketing equipment and an oxygen analyzer and alarm. Air leaked into the unit and was not detected, and an explosion occurred [43].

An unusual case of inadvertent reconnection occurred when a contract electrician pulled a cable, and it came out of the junction box. He thought he had pulled it loose, so he replaced it, but it had been deliberately disconnected [41].

1.2 IDENTIFICATION

1.2.1 The Need for Tagging

On many occasions the wrong pipeline or piece of equipment has been broken into. For example:

(a) A joint that had to be broken was marked with chalk. The mechanic broke another joint that had an old chalk mark on it. He was splashed with a corrosive chemical.

(b) An out-of-service pipeline was marked with chalk at the point where it was to be cut. Before the mechanic could start work, a heavy rain washed off the chalk mark. The mechanic "remembered" where the chalk mark had been. He was found cutting his way with a hacksaw through a line containing a hazardous chemical.

(c) Water was dripping from a joint on a line on a pipebridge. Scaffolding was erected to provide access for repair. But to avoid having to climb up onto the scaffold, the process foreman pointed out the leaking joint from the ground and asked a mechanic to remake the joint in the "water line." The joint was actually in a carbon monoxide line. So when the mechanic broke the joint he was overcome and, because of the poor access, was rescued only with difficulty.

If the process foreman had gone up to the joint on the pipebridge to fit an identifying tag, he would have realized that the water was dripping out of the carbon monoxide line.

(d) The bonnet had to be removed from a steam valve. It was pointed out to the mechanic from the floor above. He went down a flight of stairs, approached the valve from the side, and removed the bonnet from a compressed air valve. It flew off, grazing his face.

(e) Six slip-plates were inserted to isolate a tank for entry. When the work inside the tank was complete, six slip-plates were removed. Unfortunately, one of those removed was a permanent slip-plate left in position to prevent contamination. One of the temporary slip-plates was left behind.

(f) A mechanic was asked to repair autoclave No. 3. He removed the top manhole cover and then went down to the floor below to remove a manhole cover there. Instead of removing the cover from the manhole on autoclave No. 3, he removed the cover from No. 4, which contained vinyl chloride and nitrogen at a gauge pressure of 70 psi (5

bar). Polymer had formed around the inside of the manhole, so when he removed the bolts, there was no immediate evidence of pressure inside the vessel. Almost immediately afterward the pressure blew off the cover. The mechanic and two other men were blown to the ground and killed, and the vinyl chloride was ignited [23].

(g) When a man tried to start the building ventilation fans, he found that the control and power panels had been removed. Contractors were removing surplus equipment and thought that these panels were supposed to be removed. The surplus equipment should have been clearly marked [44].

(h) A section of a chlorine gas line had been renewed and had to be heat-treated. The operator who was asked to prepare the line and issue the permit-to-work misunderstood his instructions and thought a vent line had to be treated. There would be no need to gas-free this line, and he allowed the work to go ahead. It went ahead, on the correct line; the chlorine reacted with the iron, a 0.5 m length burned away, and 350 kg of chlorine escaped. To quote from the report, "at no stage on the day of the incident was the job thoroughly inspected by the issuer [of the permit-to-work] or the plant manager [supervisor in most U.S. companies]." The plant manager had inspected the permit and the heat treatment equipment but did not visit the site. He saw no reason to doubt the operator's belief that the line to be treated was the vent line [45]. Tagging would have prevented heat treatment of a line full of chlorine.

Incidents like these and many more could be prevented by fitting a numbered tag to the joint or valve and putting that number on the work permit. In incident (c), the foreman would have had to go up onto the scaffold to fix the tag. Accidents have occurred, however, despite tagging systems.

In one plant a mechanic did not check the tag number and broke a joint that had been tagged for an earlier job; the tag had been left in position. Tags should be removed when jobs are complete.

In another plant the foreman allowed a planner to fix the tags for him and did not check that they were fixed to the right equipment. The foreman prepared one line for maintenance, but the tags were on another.

1.2.2 The Need for Clear, Unambiguous Labeling

(a) A row of pumps was labeled as shown in Figure 1-7. A mechanic was asked to repair No. 7. Not unreasonably, he assumed that No. 7

Figure 1-7. Numbering pumps like this leads to error.

was the end one. He did not check the numbers. Hot oil came out of the pump when he dismantled it.

(b) There were four crystallizers in a plant, three old ones and one just installed. A man was asked to repair A. When he went onto the structure, he saw that two were labeled B and C but the other two were not labeled. He assumed that A was the old unlabeled crystallizer and started work on it. Actually, A was the new crystallizer. The original three were called B, C, and D. Crystallizer A was reserved for a possible future addition for which space was left (Figure 1-8).

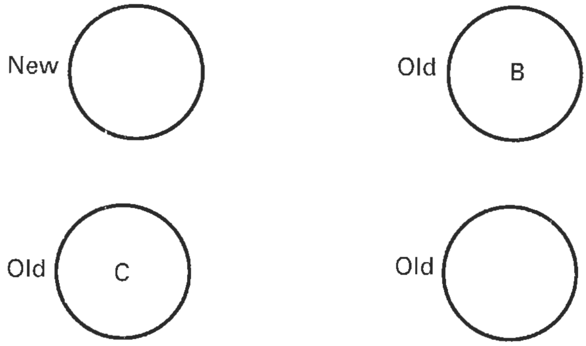


Figure 1-8. Which is crystallizer A?

(c) The labels on two air coolers were arranged as shown in Figure 1-9. The B label was on the side of the B cooler farthest away from the B fan and near the A fan. Not unreasonably, workers who were asked to overhaul the B fan assumed it was the one next to the B label and overhauled it. The power had not been isolated. But fortunately, the overhaul was nearly complete before someone started the fan.

(d) Some pump numbers were painted on the coupling *guards*. Before long, repairs were carried out on the couplings of two adjacent pumps. You can guess what happened. Now, the pump numbers are painted on the pump bodies. It would be even better to paint the numbers on the plinths.

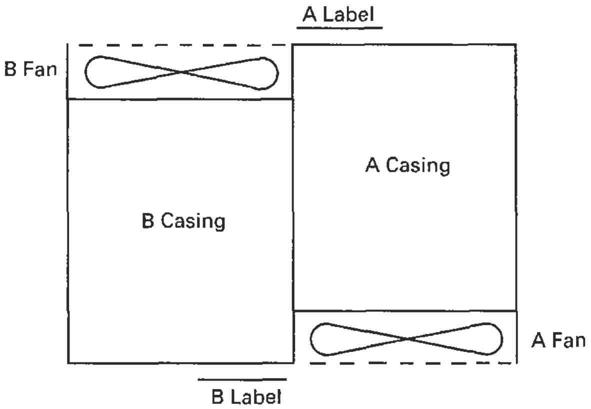


Figure 1-9. Which is the A fan?

(e) On one unit the pumps and compressors were numbered J1001 onward. When the unit's allocation of numbers was used up, numbers from JA1001 onward were used. J1001 and JA1001 sound alike (say them aloud). An operator was asked to prepare JA1001—a small pump—for repair. He thought the foreman said J1001 and went to it. J1001 was a 40,000 HP compressor. Fortunately, the size of the machine made him hesitate. He asked the foreman if he really wanted the compressor shut down.

1.2.3 The Need for Clear Instructions

(a) A permit was issued for modifications to the walls of a room. The maintenance workers started work on the ceilings as well and cut through live electric cables.

(b) A permit was issued for welding on the top only of a tank, which had been removed from the plant. When the job was complete, the welders rolled the tank over so that another part became the top. Some residue, which had been covered by water, caught fire.

(c) Because a lead operator on a chlorine storage unit was rather busy, he asked the second operator to issue a permit for heat treatment of a line. The second operator misunderstood his instructions and issued a permit for the wrong line. The lead operator's supervisor checked the permit and inspected the heat treatment equipment but did not look at the line. The line actually heat-treated contained chlorine, and the

heat was sufficient for the iron and the chlorine to react and "burn" a hole in the line; 350 kg of chlorine escaped. Afterward, the lead operator said he thought it was obvious that the line to be heat-treated was the one that had been renewed the day before [24].

(d) An electrician was asked, in writing, to remove a fuse labeled FU-5. He did so. Unfortunately, he removed a fuse labeled FU-5 from the fuseboard that supplied the control room, not from the fuseboard that supplied the equipment room [25]. Not only were his instructions ambiguous, but the labeling system was poor.

(e) An operator asked an electrician to disconnect the cable leading to a piece of equipment that was to be modified. The operator checked the disconnection and signed the permit-to-work for the modification. A second operator certified that that preparation had been carried out correctly.

The construction worker who was to carry out the modification checked the cable with a current detector and found that the wrong one had been disconnected. It was then found that the cable was incorrectly described on the written instructions given to the operators. The description of the cable was not entirely clear, but instead of querying it, the first operator decided what he thought was the correct cable and asked the electrician to disconnect it. The second operator, or checker, had not been trained to check cables [32].

This incident shows the weakness of checking procedures. The first operator may assume that if anything is wrong the checker will pick it up; the checker may become casual because he has never known the first operator to make an error (see Sections 3.2.7 b and 14.5 c).

1.2.4 Identification of Relief Valves

Two relief valves, identical in appearance, were removed from a plant during a shutdown and sent to the workshops for overhaul. One relief valve was set to operate at a gauge pressure of 15 psi (1 bar) and the other at 30 psi (2 bar). The set pressures were stamped on the flanges, but this did not prevent the valves from being interchanged.

A number of similar incidents have occurred in other plants.

Such incidents can be prevented, or at least made much less likely, by tying a numbered tag to the relief valve when it is removed and tying another tag with the same number to the flange.

1.2.5 Make Sure You Find the Right Line

There was a leak on the line supplying steam to a plant. To avoid a shutdown, a hot tap and stopple was carried out, that is, the line was bypassed and the leaking section plugged off (stoppled) while in use. The job went well mechanically, but the leak continued. It was then found that the leak was not coming from the steam line but from a hot condensate line next to it. The condensate flashed as it leaked, and the leak looked like a steam leak [26].

1.3 REMOVAL OF HAZARDS

Many accidents have occurred because equipment, though isolated correctly, was not completely freed from hazardous materials or because the pressure inside it was not completely blown off and the workers carrying out the repair were not made aware of this.

1.3.1 Equipment Not Gas-freed

It is usual to test for the presence of flammable gas or vapor with a combustible gas detector before maintenance, especially welding or other hot work, is allowed to start. The following incidents show what can happen if these tests are not carried out or not carried out thoroughly. Large pieces of equipment or those of complex shape should be tested in several places, using detector heads at the ends of long leads if necessary (see Section 5.4.2 d).

(a) An explosion occurred in a 4,000-m^3 underground storage tank at Sheffield Gas Works, England, in October 1973. Six people were killed, 29 injured, and the tank was destroyed. The tank top was thrown into the air, turned over, and deposited upside down on the bottom of the tank.

The tank had contained a light naphtha and had not been thoroughly cleaned before repairs started. It had been filled with water and then emptied, but some naphtha remained in various nooks and crannies. (It might, for example, have gotten into the hollow roof supports through pinholes or cracks and then drained out when the tank was emptied.) No tests were carried out with combustible gas detectors.

It is believed that the vapor was ignited by welding near an open vent. The body of the welder was found 100 ft up on the top of a neighboring gasholder, still holding a welding torch.

According to the incident report, there was no clear division of responsibilities between the Gas Board and the contractor who was carrying out the repairs. "Where, as in this case, a special risk is likely to arise due to the nature of the work performed (and the owner of the premises has special knowledge of it), the owner must retain sufficient control of the operation to ensure that contractors' employees are properly protected against the risk" [4].

(b) A bottom manhole was removed from an empty tank still full of gasoline vapor. Vapor came out of the manhole and caught fire. As the vapor burned, air was sucked into the tank through the vent until the contents became explosive. The tank then blew up [5].

(c) Welding had to be carried out—during a shutdown—on a relief valve tailpipe. It was disconnected at both ends. Four hours later the atmosphere at the end farthest from the relief valve was tested with a combustible gas detector. The head of the detector was pushed as far down the tailpipe as it would go; no gas was detected, and a work permit was issued. While the relief valve discharge flange was being ground, a flash and bang occurred at the other end of the tailpipe. Fortunately, no one was hurt. Gas in the tailpipe—20 m long and containing a number of bends—had not dispersed and had not been detected by a test at the other end of the pipe.

Before allowing welding or similar operations on a pipeline that has or could have contained flammable gas or liquid, (1) sweep out the line with steam or nitrogen from end to end, and (2) test at the point at which welding will be carried out. If necessary, a hole may have to be drilled in the pipeline.

(d) Solids in a vessel can "hold" gas that is released only slowly. A reactor, which contained propylene and a layer of polypropylene granules 1–1.5 m thick, had to be prepared for maintenance. It was purged with nitrogen six times. A test near the manhole showed that only a trace of propylene was present, less than 5% of the lower explosive limit (LEL). However, when the reactor was filled with water, gas was emitted, and gas detectors in the surrounding area registered 60% of the LEL.

The vessel had been prepared for maintenance in a similar way on three previous occasions, but there was then far fewer granules in the reactor [14] (see Section 11.1 a and b).

(e) A label had to be welded onto an empty drum. As the drum was brand new, no precautions were taken, and no tests were carried out. The drum exploded, breaking the welder's leg. The manufacturer had cleaned the drum with a flammable solvent, had not gas-freed it, and had not warned the customer [15].

(f) In 1992, the catwalks and ladders were being removed with oxy-acetylene torches from a group of tanks so the tanks could be moved. An empty tank that had contained ethanol exploded, killing three men. The ethanol vapor had leaked out of a faulty seal on the gauge hatch; it was ignited by a torch, and the flame traveled back into the tank. The men who were killed had taken combustible gas detectors onto the job, but no one knew whether they had used them correctly or had used them at all. Gas testing should be carried out by the operating team before it issues a permit-to-work; since the tanks would have had to be gas-freed before they were moved, this should have been done before hot work started [27].

(g) In fluidized bed catalytic cracker units, air is blown into large vessels called regenerators to burn carbon off the catalyst. The regenerators are vented to the air, so there should be no need to test or inert them before maintenance. However, on one occasion when a manway cover was being removed, 50 hours after the unit had shut down, an explosion occurred inside the vessel, and flames appeared at various openings in the ducts connected to it.

Carbon is usually burnt off before a shutdown. On this occasion the air blower failed, and the unit had to shut down at once. Steam was blown into the regenerator, and most of the catalyst was removed. However, the steam reacted with the carbon on the remaining catalyst, forming hydrogen and carbon monoxide. When the manway cover was removed, air entered the regenerator, and an explosion occurred. The source of ignition was the hot catalyst, which was still at about 600°C [33]. Older regenerators are fitted with a spare blower. Some plants connect up mobile blowers if their single blower fails.

This incident shows the importance, during hazard and operability studies (see Chapter 18), of considering abnormal conditions, such as failure of utilities, as well as normal operation.

1.3.2 Conditions Can Change After Testing

As already stated, it is usual to test for the presence of flammable gas or vapor with a combustible gas detector before maintenance, especially welding or other hot work, starts. Several incidents have occurred because tests were carried out several hours beforehand and conditions changed.

(a) An old propylene line that had been out of use for 12 years had to be modified for reuse. For the last two years it had been open at one end and blanked at the other. The first job was welding a flange onto the open end. This was done without incident. The second job was to fit a 1-in. branch 60 m from the open end. A hole was drilled in the pipe and the inside of the line tested. No gas was detected. Fortunately, a few hours later, just before welding was about to start, the inside of the pipe was tested again, and flammable gas was detected. It is believed that some gas had remained in the line for 12 years and a slight rise in temperature had caused it to move along the pipeline. Some people might have decided that a line out of use for 12 years did not need testing at all. Fortunately, the men concerned did not take this view. They tested the inside of the line and tested again immediately before welding started.

(b) A test for benzene in the atmosphere was carried out eight hours before a job started. During this time the concentration of benzene rose.

(c) An acid tank was prepared for welding and a permit issued. The maintenance team was not able to start for 40 days. During this time a small amount of acid that had been left in the tank attacked the metal, producing hydrogen. No further tests were carried out. When welding started, an explosion occurred [6].

(d) A branch had to be welded onto a pipeline that was close to the ground. A small excavation, between ½ and 1 m deep, was made to provide access to the bottom of the pipeline. The atmosphere in the excavation was tested with a combustible gas detector, and because no gas was detected, a welding permit was issued. Half an hour later, after the welder had started work, a small fire occurred in the excavation. Some hydrocarbons had leaked out of the ground. This incident shows that it may not be sufficient to test just before welding starts. It may be necessary to carry out continuous tests using a portable combustible gas detector alarm.

(e) The sewer from a chemical plant discharged into a river. The river wall was lined with steel plates, and a welder was burning holes in one of them, just downstream of the outlet, so that it could be removed by a crane. The atmosphere was tested for flammable gas before work started. After a break the welder started again. There was a flash fire, which did not last long but killed the welder. An underground pipeline was leaking, and it seems that the liquid had collected in a sump and then overflowed into the sewer.

Section 11.5 describes another fatality caused by hazardous materials in drains.

1.3.3 Hazards Can Come Out of Drains, Vents, and Other Openings

A number of incidents have occurred because gas or vapor came out of drains or vent while work was in progress. For example:

(a) Welding had to be carried out on a pipeline 6 m above the ground. Tests inside and near the pipeline were negative, and so a work permit was issued. A piece of hot welding slag bounced off a pipeline and fell onto a sump 6 m below and 2.5 m to the side. The cover on the sump was loose, and some oil inside caught fire. Welding jobs should be boxed in with fire-resistant sheets. Nevertheless, some sparks or pieces of slag may reach the ground. So drains and sumps should be covered.

(b) While an electrician was installing a new light on the outside wall of a building, he was affected by fumes coming out of a ventilation duct 0.6 m away. When the job was planned, the electrical hazards were considered and also the hazards of working on ladders. But it did not occur to anyone that harmful or unpleasant fumes might come out of the duct. Yet ventilation systems are installed to get rid of fumes.

(c) Radioactive material was transferred into transport casks by remote handling in a shielded cell. Checks showed that the radiation level outside the cell was low, but no one thought about the roof. Several years later, a technician walked across the flat roof while a transfer was taking place below. Fortunately she was carrying a radiation detector, and when it alarmed, she left at once. The radiation stream to the roof was greater than 50 mSv/hr, and the technician received a dose of about 1 mSv. (The International Committee on Radiological Protection recommends that no one be exposed to more than 50 mSv in a single year or more than 20 mSv/yr (2 rem/yr) averaged

over five years. In practice most radiation workers receive far smaller doses.) Several similar incidents have been reported [34].

Not many readers will handle radioactive materials, but this incident and the previous one do show how easy it is to overlook some of the routes by which hazardous materials or effects can escape from containment.

1.3.4 Liquid Can Be Left in Lines

When a line is drained or blown clear, liquid may be left in low-lying sections and run out when the line is broken. This is particularly hazardous if overhead lines have to be broken. Liquid splashes down onto the ground. Funnels and hoses should be used to catch spillages.

When possible, drain points in a pipeline should be fitted at low points, and slip-plates should be fitted at high points.

1.3.5 Service Lines May Contain Hazardous Materials

Section 1.1.4 described how fumes got into a steam drum because it was not properly isolated. Even when service lines are not directly connected to process materials, they should always be tested before maintenance, particularly if hot work is permitted on them, as the following incidents show:

(a) A steam line was blown down and cold cut. Then a plug was hammered into one of the open ends. A welder struck an arc ready to weld in the plug. An explosion occurred, and the plug was blown out of the pipeline, fortunately missing the welder. Acid had leaked into the pipeline through a corroded heating coil in an acid tank and had reacted with the iron of the steam pipe, producing hydrogen.

(b) While a welder was working on the water line leading to a waste heat boiler, gas came out of a broken joint and caught fire. The welder was burned but not seriously. There was a leaking tube in the waste heat boiler. Normally, water leaked into the process stream. However, on shutting down the plant, pressure was taken off the water side before it was taken off the process side, thus reversing the leak direction. The water side should have been kept up to pressure until the process side was depressured. In addition, the inside of the water lines should have been tested with a combustible gas detector.

See also Section 5.4.2 (b).

1.3.6 Trapped Pressure

Even though equipment is isolated by slip-plates and the pressure has been blown off through valves or by cracking a joint, pressure may still be trapped elsewhere in the equipment, as the following incidents show:

(a) This incident occurred on an all-welded line. The valves were welded in. To clear a choke, a fitter removed the bonnet and inside of a valve. He saw that the seat was choked with solid and started to chip it away. As he did so, a jet of corrosive chemical came out under pressure from behind the solid, hit him in the face, pushed his goggles aside, and entered his eye.

(b) An old acid line was being dismantled. The first joint was opened without trouble. But when the second joint was opened, acid came out under pressure and splashed the fitter and his assistant in their faces. Acid had attacked the pipe, building up gas pressure in some parts and blocking it with sludge in others.

(c) A joint on an acid line, known to be choked, was carefully broken, but only a trickle of acid came out. More bolts were removed, and the joint pulled apart, but no more acid came. When the last bolt was removed and the joint pulled wide apart, a sudden burst of pressure blew acid into the fitter's face.

In all three cases the lines were correctly isolated from operating equipment. Work permits specified that goggles should be worn and stated, "Beware of trapped pressure."

To avoid injuries of this sort, we should use protective hoods or helmets when breaking joints on lines likely to contain corrosive liquids trapped under pressure, either because the pressure cannot be blown off through a valve or because lines may contain solid deposits.

Other incidents due to trapped pressure and clearing chokes are described in Sections 17.1 and 17.2.

1.3.7 Equipment Sent Outside the Plant

When a piece of equipment is sent to a workshop or to another company for repair or modification we should, whenever possible, make sure that it is spotlessly clean before it leaves the plant. Contractors are usually not familiar with chemicals and do not know how to handle them.

Occasionally, however, it may be impossible to be certain that a piece of equipment is spotlessly clean, especially if it has contained a residual oil or a material that polymerizes. If this is the case, or if there is some doubt about its cleanliness, then the hazards and the necessary precautions should be made known to the workshop or the other company. This can be done by attaching a certificate to the equipment. This certificate is not a work permit. It does not authorize any work but describes the state of the equipment and gives the other company sufficient information to enable it to carry out the repair or modification safely. Before issuing the certificate, the engineer in charge should discuss with the other company the methods it proposes to use. If the problems are complex, a member of the plant staff may have to visit the other company. The following incidents show the need for these precautions.

(a) A large heat exchanger, 2.4 m long by 2.6 m diameter, was sent to another company for retubing. It contained about 800 tubes of 2½-in. diameter and about 80 of these tubes had been plugged. The tubes had contained a process material that tends to form chokes, and the shell had contained steam.

Before the exchanger left the plant, the free tubes were cleaned with high-pressure water jets. The plugged tubes were opened up by drilling ⅜-in. holes through the plugs to relieve any trapped pressure. But these holes were not big enough to allow the tubes to be cleaned.

A certificate was attached to the exchanger stating that welding and burning were allowed but only to the shell. The contractor, having removed most of the tubes, decided to put workers into the shell to grind out the plugged tubes. He telephoned the plant and asked if it would be safe to let workers enter the shell. He did not say why he wanted them to do so.

The plant engineer who took the telephone call said that the shell side was clean and therefore entering it would be safe. He was not told that the workers were going into it to grind out some of the tubes.

Two men went into the shell and started grinding. They were affected by fumes, and the job was left until the next day. Another three workers then restarted the job and were affected so badly that they were hospitalized. Fortunately, they soon recovered.

The certificate attached to the exchanger when it left the plant should have contained much more information. It should have said that the plugged tubes had not been cleaned and that they contained a chemical that gave off fumes when heated. Better still, the plugged tubes should have been opened up and cleaned. The contractor would have to remove the plugs, so why not remove them before they left the plant?

(b) At least two serious titanium fires have occurred when scrap metal dealers used torches to cut up heat exchangers containing titanium tubes [28]. Once titanium (melting point about 1660°C) is molten, it burns readily in air. Titanium sent for scrap should be clearly labeled with a warning note.

Do your instructions cover the points mentioned in this section?

1.4 PROCEDURES NOT FOLLOWED

It is usual, before a piece of equipment is maintained, to give the maintenance team a permit-to-work that sets out:

1. What is to be done.
2. How the equipment is isolated and identified.
3. What hazards, if any, remain.
4. What precautions should be taken.

This section describes incidents that occurred because of loopholes in the procedure for issuing work permits or because the procedure was not followed. There is no clear distinction between these two categories. Often the procedure does not cover, or seem to cover, all circumstances. Those concerned use this as the reason, or excuse, for a shortcut, as in the following two incidents:

1.4.1 Equipment Used After a Permit has Been Issued

(a) A plumber foreman was given a work permit to modify a pipeline. At 4 p.m. the plumbers went home, intending to complete the job on the following day. During the evening the process foreman wanted to use the line the plumbers were working on. He checked that the line was safe to use, and he asked the shift maintenance

man to sign off the permit. Next morning, the plumbers, not knowing that their permit had been withdrawn, started work on the line while it was in use.

To prevent similar incidents from happening, (1) it should be made clear that permits can only be signed off by the person who has accepted them (or a person who has taken over that person's responsibilities), and (2) there should be two copies of every permit, one kept by the maintenance team and one left in the book in the process team's possession.

(b) A manhole cover was removed from a reactor so some extra catalyst could be put in. After the cover had been removed, it was found that the necessary manpower would not be available until the next day. So it was decided to replace the manhole cover and regenerate the catalyst overnight. By this time it was evening, and the maintenance foreman had gone home and left the work permit in his office, which was locked. The reactor was therefore boxed up and catalyst regeneration carried out with the permit still in force. The next day a fitter, armed with the work permit, proceeded to remove the manhole cover again and, while doing so, was drenched with process liquid. Fortunately, the liquid was mostly water, and he was not injured.

The reactor should not have been boxed up and put on line until the original permit had been handed back. If it was locked up, then the maintenance supervisor should have been called in. Except in an emergency, plant operations should never be carried out while a work permit is in force on the equipment concerned.

1.4.2 Protective Clothing Not Worn

The following incidents are typical of many:

(a) A permit issued for work to be carried out on an acid line stated that goggles must be worn. Although the line had been drained, there might have been some trapped pressure (see Section 1.3.6). The man doing the job did not wear goggles and was splashed in the eye.

At first, it seemed the injury was entirely the fault of the injured man and no one else could have done anything to prevent it. However, further investigation showed that all permits issued asked for

goggles to be worn, even for repairs to water lines. The maintenance workers therefore frequently ignored this instruction, and the managers turned a blind eye. No one told the fitter that on this job, goggles were really necessary.

It is bad management for those issuing work permits to cover themselves by asking for more protective clothing than is really necessary. They should ask only for what is necessary and then *insist* that it be worn.

Why did they ask for more than was necessary in this case? Perhaps someone was reprimanded because he asked for less protective clothing than his supervisor considered necessary. That person and his colleagues then decided to cover themselves by asking for everything every time. If we give people the discretion to decide what is necessary, then inevitably they will at times come to a different decision than we would. We may discuss this with them but should not reprimand them.

(b) Two men were told to wear air masks while repairing a compressor, which handled gas containing hydrogen sulfide. The compressor had been swept out, but traces of gas might have been left in it. One of the men had difficulty handling a heavy valve that was close to the floor and removed his mask. He was overcome by gas—hydrogen sulfide or possibly nitrogen.

Again, it is easy to blame the man. But he had been asked to do a job that was difficult to perform while wearing an air mask. The plant staff members resisted the temptation to blame him—the easy way out. Instead, they looked for suitable lifting aids [7].

Section 3.2 discusses similar incidents. Rather than blame workers who make mistakes or disobey instructions, we should try to remove the opportunities for error by changing the work situation, that is, the design or method of operation.

(c) Work permits asked for goggles to be worn. They were not always worn and, inevitably, someone was injured. This incident differs from (a) in that goggles were always necessary on this unit.

Investigation showed that the foreman and manager knew that goggles were not always worn. But they turned a blind eye to avoid dispute and to avoid delaying the job. The workers knew this and said to themselves, "Wearing goggles cannot be important." The foreman and manager were therefore responsible for the inevitable injury.

People doing routine tasks become careless. Foremen and managers cannot be expected to stand over them all the time, but they can make occasional checks to see that the correct precautions are taken. And they can comment when they see rules being flouted. A friendly word *before* an accident is better than punitive action afterward.

1.4.3 Jobs Near Plant Boundaries

Before a permit to weld or carry out other hot work is issued, it is normal practice to make sure there are no leaks of flammable gas or liquid *nearby* and no abnormal conditions that make a leak likely. The meaning of nearby depends on the nature of the material that might leak, the slope of the ground, and so on. For highly flammable liquids, 15 m is often used.

Fires have occurred because a leak in one unit was set alight be welding in the unit next door. Before welding or other hot work is permitted within 15 m, say, of a unit boundary, the foreman of the unit next door should countersign it.

Similar hazards arise when a pipeline belonging to one unit passes through another unit.

Suppose a pipeline belonging to area A passes through area B and that this pipeline has to be broken in area B (Figure 1-10).

The person doing the job is exposed to two distinct hazards: those due to the contents of the pipeline (these are understood by area A foreman) and those due to work going on in area B (these are understood by area B foreman). If the work permit for the pipeline is issued by area A foreman, then area B foreman should countersign it. If it is issued by B, then A

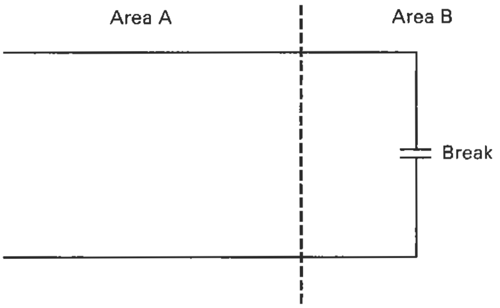


Figure 1-10. Who should authorize the pipeline break?

should countersign it. The system should be covered by local instructions and clearly understood.

An incident occurred because area A foreman issued a permit for work to be done on a flow transmitter in a pipeline in area B. Area B foreman issued a permit for grinding in area B. He checked that no flammable gas was present and had the drains covered. He did not know about the work on the flowmeter. A spark set fire to a drain line on the flowmeter, which had been left open.

What would happen in your plant?

1.4.4 Maintenance Work Over Water

A welder was constructing a new pipeline in a pipe trench, while 20 m away a slip-plate was being removed from another pipe, which had contained light oil. Although the pipe had been blown with nitrogen, it was realized that a small amount of the oil would probably spill when the joint was broken. But it was believed that the vapor would not spread to the welders. Unfortunately, the pipe trench was flooded after heavy rain, and the oil spread across the water surface and was ignited by the welder's torch. One of the men working on the slip-plate 20 m away was badly burned and later died.

The first lesson from the incident is that *welding should not be allowed over large pools of water.* Spillages some distance away might be ignited. In 1970, 35 tons of gasoline were spilled on the Manchester Ship Canal, England; 1 km away, 2½ hours later, the gasoline caught fire, killing six men [8].

The second lesson is that *when large joints have to be broken regularly, a proper means of draining the line should be provided.* The contents should not be allowed to spill onto the ground when the joint is broken.

Why was a permit issued to remove a slip-plate 20 m away from a welding job? Although vapor should not normally spread this far, the two jobs were rather close together.

The foremen who issued the two permits were primarily responsible for operating a unit some distance away. As they were busy with the running plant, they did not visit the pipe trench as often as they might. Had they visited it immediately before allowing the de-slip-plating job to start, they would have realized that the two jobs were close together. They might have realized that oil would spread across the water in the trench.

After the incident, special day foremen were appointed to supervise construction jobs and interface with the construction teams. The construction teams like this system because they deal with only one process foreman instead of four shift foremen.

For another incident involving a construction team, see Section 5.4.2 (b).

1.4.5 Misunderstandings

Many incidents have occurred because of misunderstandings of the meanings of words and phrases. The following incidents are typical:

(a) A permit was issued to remove a pump for overhaul. The pump was defused, removed, and the open ends blanked. The next morning the maintenance foreman signed the permit to show that the job—removing the pump—was complete. The morning shift lead operator glanced at the permit. Seeing that the job was complete, he asked the electrician to replace the fuses. The electrician replaced them and signed the permit to show that he had done so. By this time the afternoon shift lead operator had come on duty. He went out to check the pump and found that it was not there.

The job on the permit was to remove the pump for overhaul. Permits are sometimes issued to remove a pump, overhaul it, and replace it. But in this case the permit was just for removal (see Section 1.1.2). When the maintenance foreman signed the permit to show that the job was complete, he meant that the job of *removal* was complete. The lead operator, however, did not read the permit thoroughly. He assumed that the *overhaul* was complete.

The main message is clear: read permits carefully; don't just glance at them.

When a maintenance worker signs a permit to show that the job is complete, he means he has completed the job *he thought he had to do.* This may not be the same as the job he was expected to do. The job should therefore always be inspected by the process team to make sure that the one completed is the one wanted.

When handing over or handing back a permit, the maintenance and process people should speak to each other. It is not good practice to leave a permit on the table for someone to sign when he comes in.

(b) When a work permit is issued to excavate the ground, it is normal practice for an electrician to certify that there are no buried cables. What, however, is an excavation? A contractor asked for and received a work permit to "level and scrape the ground." No excavation was requested, so the process foreman did not consult the electricians. The contractor used a mechanical shovel, removed several feet of dirt from the ground, and cut through a live electric cable. The word *excavation* needs careful definition.

(c) A construction worker was wearing a plastic protective suit, supplied by breathing air, when the air supply suddenly stopped. Fortunately, he was rescued without injury. A mechanic had isolated the breathing air supply to change a filter.

The plant had what everyone involved thought was a good system: before anyone used breathing air or did any work on the air system, that person was supposed to tell the control room. Unfortunately, the supervisor and the stand-by operator both thought that the other was going to do so. The mechanic did contact the control room before starting work, but the control room staff told him that no one was using breathing air. To make sure, both the mechanic and someone from the control room had a look around, but the check was rather casual as neither of them expected to find anyone. The air was in use in an out-of-the-way part of the site, and neither of them noticed the job [29].

This system of working was not really very good. No work should be allowed on the breathing air system (or any other system) without a permit-to-work, as people will say OK with less thought than they will sign a form. Users of breathing air should sign a book in the control room or collect a tag, not just tell someone they are going to use the air.

(d) Electricity supplies to a boiler and a water treatment unit were isolated for replacement of electrical equipment. The supervisor in charge of the work kept in touch with the two units by radio. After the replacement work had been carried out, he received a message that testing was complete. The message actually said that the testing on the water treatment unit was complete, but the supervisor took it to mean that testing on both units was complete. He therefore announced over his radio that power would be restored to both units. The crew working on the boiler plant did not hear this message and continued testing. When power was restored, arcing occurred at a test point on the boiler plant. Fortunately the electri-

cian carrying out the test was wearing high-voltage gloves and safety glasses, or he might have been killed [35].

The report says that when communicating by radio, no action should be taken until the message has been acknowledged, but this is nowhere near sufficient. Power should not have been restored until the crews working on both units had signed off written permits-to-work. Verbal communication alone is never adequate.

(e) While someone was writing out a permit-to-work in duplicate, the lower copy moved under the carbon paper, and a wrong line was crossed out on the lower copy. It was given to the man who was to repair the equipment, and as a result of the error he thought the plant was free from acid. While he was breaking a joint, sulfuric acid came out and burnt him on the face and neck [46].

1.4.6 Excavations

A report from the U.S. Department of Energy (DOE) says that events involving the unexpected discovery of underground utilities during excavations or trenching operations have occurred at its facilities [36]. Several of the events resulted in electric shock; one caused serious injury, and many others were near-misses. The serious injury occurred when a sump 1 m deep was being constructed in the basement of a building, and a compressed air hammer hit a 13,200-volt power line. Before any excavation (or leveling of the ground; see Section 1.4.5 b) is authorized, the electrical department should certify that no electric cables are present or that any present have been isolated. If any underground pipelines are present, they should be identified, from drawings or with metal detectors, and excavations nearby (say, within 1 m) should be carried out by hand.

In another incident a backhoe ruptured a 3-in. polyethylene natural gas pipeline; fortunately the gas did not ignite. The drawings were complex and cluttered, and the contractor overlooked the pipeline. A metal detector was not used. This would have detected the pipe as a metal wire was fixed to it, a good practice. In a third incident a worker was hand-digging a trench, as an electric conduit was believed to be present. It was actually an old transfer line for radioactive waste, and he received a small dose of radioactivity. The planner had misread the drawing.

1.4.7 A Permit to Work Dangerously?

A permit system is necessary for the safe conduct of maintenance operations. But issuing a permit in itself does not make the job safe. It merely provides an opportunity to check what has been done to make the equipment safe, to review the precautions necessary, and to inform those who will have to carry out the job. The necessity of saying this is shown by the following quotation from an official report:

> ". . . they found themselves in difficulty with the adjustment of some scrapers on heavy rollers. The firm's solution was to issue a work permit, but it was in fact a permit to live dangerously rather than a permit to work in safety. It permitted the fitter to work on the moving machinery with the guards removed. A second permit was issued to the first aid man to enable him to stand close to the jaws of death ready to extricate, or die in the attempt to extricate, the poor fitter after he was dragged into the machinery. In fact, there was a simple solution. It was quite possible to extend the adjustment controls outside the guard so that the machinery could be adjusted, while still in motion, from a place of safety" [9].

1.5 QUALITY OF MAINTENANCE

Many accidents have occurred because maintenance work was not carried out in accordance with the (often unwritten) rules of good engineering practice, as the following incidents and Section 10.4.5 show.

1.5.1 The Right and Wrong Ways to Break a Joint

(a) One of the causes of the fire described in Section 1.1.1 was the fact that the joint was broken incorrectly. The fitter removed all the nuts from the pump cover and then used a wedge to release the cover, which was held tightly on the studs. It came off suddenly, followed by a stream of hot oil.

The correct way to break a joint is to slacken the nuts farthest away from you and then spring the joint faces apart, using a wedge if necessary. If any liquid or gas is present under pressure, then the pressure can be allowed to blow off slowly or the joint can be retightened.

(b) Another incident was the result of poor preparation and poor workmanship. A valve had to be changed. The valves on both sides were

closed, and a drain valve in between opened. A flow through the drain valve showed that one of the isolating valves was leaking, so the drain valve was closed and a message left for the employees working the next shift, telling them to open the drain valve before work started. Nothing was written on the permit-to-work. The message was not passed on: the drain valve was not opened, and the fitter broke the joint the wrong way, removing all the bolts. The joint blew apart, and the fitter received head injuries from which he will never fully recover [37].

(c) It is not only flammable oils that cause accidents. In another incident two workers were badly scalded when removing the cover from a large valve on a hot water line, although the gauge pressure was only 9 in. of water (0.33 psi or 0.023 bar). They removed all the nuts, attached the cover to a chain block, and tried to lift it. To release the cover they tried to rock it. The cover suddenly released itself, and hot water flowed out onto the workers' legs.

1.5.2 Use of Excessive Force

A joint on an 8-in. line containing a hot solvent had to be remade. The two sides were ¾-in. out of line. There was a crane in the plant at the time, so it was decided to use it to lift one of the lines slightly. The lifting strap pulled against a ¾-in. branch and broke it off (Figure 1-11).

It was not a good idea to use a crane for a job like this on a line full of process material. Fortunately the leaking vapor did not ignite, although

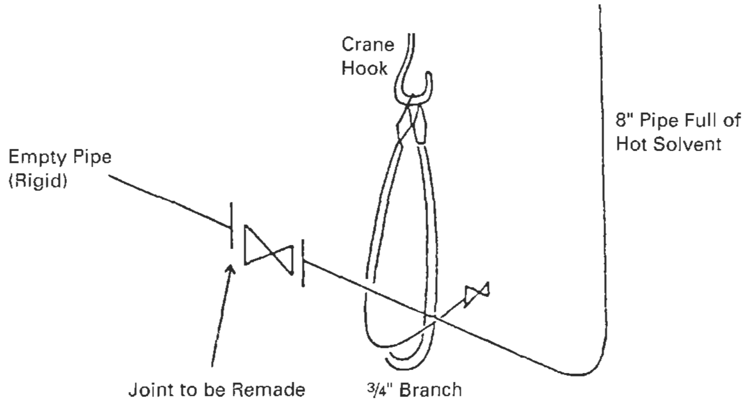


Figure 1-11. A branch broke when a crane was used to move a live line.

nearby water was being pumped out of an excavation. At one time a diesel pump would have been used, but the use of diesel pumps had been banned only a few months before the incident.

Section 2.11.1 describes an explosion caused by the failure of nuts that had been tightened with excessive force.

1.5.3 Ignorance of Material Strength

(a) When a plant came back on line after a long shutdown, some of the flanges had been secured with stud bolts and nuts instead of ordinary bolts and nuts. And some of the stud bolts were located so that more protruded on one side than on the other. On some flanges, one of the nuts was secured by only two or three threads (Figure 1-12).

Nobody knows why this had been done. Probably one nut was tighter than the other, and in attempting to tighten this nut, the whole stud was screwed through the second nut. Whatever the reason, it produced a dangerous situation because the pressure on different parts of the flange was not the same.

In addition, stud bolts should not be indiscriminately mixed with ordinary bolts or used in their place. They are often made of different grades of steel and produce a different tension.

In the plant concerned, for the eight-bolt joints the bolts were changed one bolt at a time. Four-bolt joints were secured with clamps until the next shutdown.

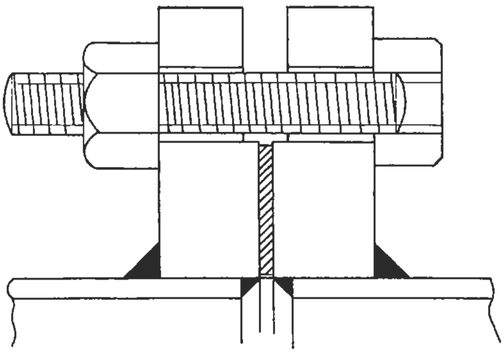


Figure 1-12. Nuts fitted incorrectly to studs.

(b) There was a leak on a large fuel-gas system operating at gasholder pressure. To avoid a shutdown, a wooden box was built around the leak and filled with concrete. It was intended as a temporary job but was so successful that it lasted for many years.

On other occasions, leaks have been successfully boxed in or encased in concrete. But the operation can only be done at low pressures, and expert advice is needed, as shown by the following incident.

There was a bad steam leak from the bonnet gasket of a 3-in. steam valve at a gauge pressure of 300 psi (20 bar). An attempt to clamp the bonnet was unsuccessful, so the shift crew decided to encase the valve in a box. Crew members made one 36 in. long, 24 in. wide, and 14 in. deep out of ¼-in. steel plate. Plate of this thickness is strong, but the shape of the box was unsuitable for pressure and could hardly have held a gauge pressure of more than 50 psi (3 bar), even if the welds had been full penetration, which they were not (Figure 1-13).

The box was fitted with a vent and valve. When the valve was closed, the box started to swell, and the valve was quickly opened.

A piece of 2-in. by 2-in. angle iron was then welded around the box to strengthen it. The vent valve was closed. A few minutes later the box exploded. Fortunately the mechanic—if he deserves the title—had moved away.

This did not happen in a back-street firm but in a major international company.

These incidents show the need for continual vigilance. We cannot assume that because we employ qualified craftsmen and graduate engineers they will never carry out repairs in a foolish or unsafe manner.

1.5.4 Failure to Understand How Things Work or How They Are Constructed

(a) Several spillages have occurred from power-operated valves while the actuators were being removed because the bolts holding the valve bonnets in position were removed in error. Figures 1-14 and 1-15 show how two such incidents occurred. The second system is particularly vulnerable because in trying to unscrew the nuts that

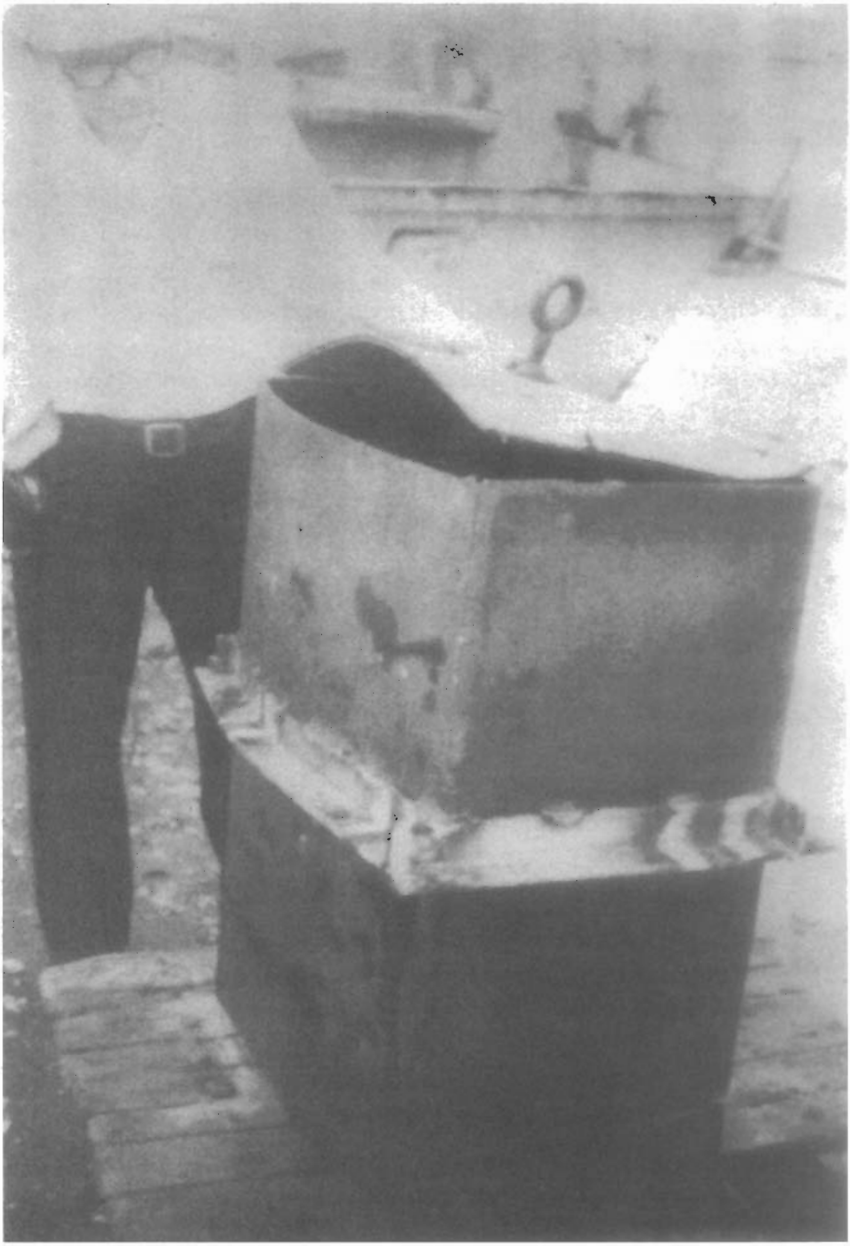


Figure 1-13. This steel box was quite incapable of containing a leak of steam at a gauge pressure of 300 psi (20 bar).

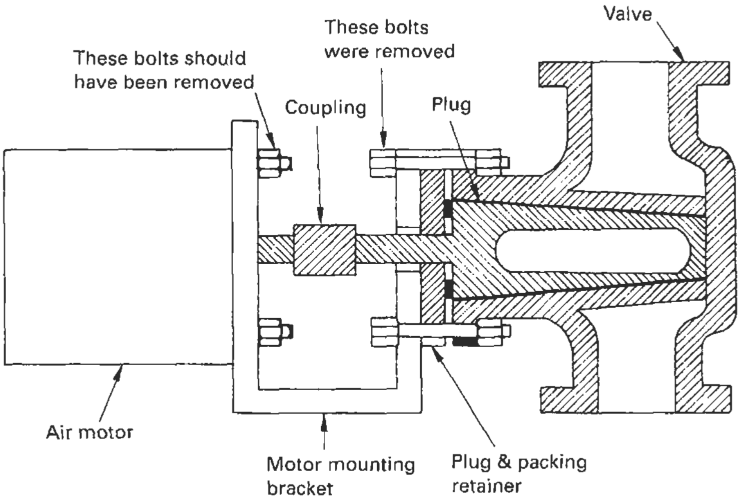


Figure 1-14. Wrong nuts undone to remove valve actuator.

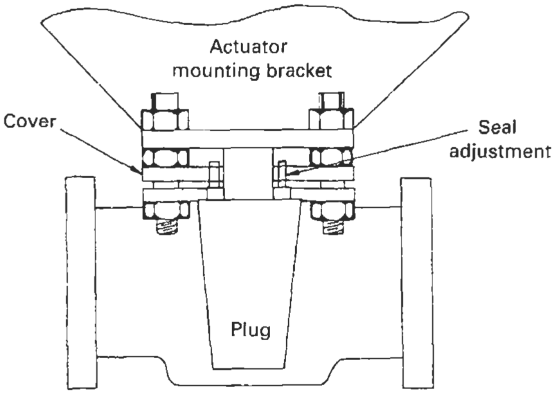


Figure 1-15. Wrong nuts undone to remove valve actuator.

hold the actuator mounting bracket in place, the stud may unscrew out of the lower nuts. This incident could be classified as due to poor design [10].

The first incident resulted in the release of 70–100 tons of vinyl chloride. There was little wind, and the cloud of vapor and mist drifted slowly backward and forward. After an hour, when the cloud was about 240 m across and 1.5 m deep, it ignited. Some of

the vinyl chloride had entered buildings, and it exploded, destroying the buildings. The rest burned outside and caused several vinyl chloride tanks to burst, adding further fuel to the fire. Remarkably, only one man was killed. The injured included spectators who arrived to watch the fire [30].

(b) A similar accident occurred on a common type of ball valve. Two workers were asked to fit a drain line below the valve. There was not much room. So they decided to remove what they thought was a distance piece or adaptor below the valve but which was in fact the lower part of the valve body (Figure 1-16). When they had removed three bolts and loosened the fourth, it got dark, and they left the job to the next day.

The valve was the drain valve on a small tank containing liquefied petroleum gas (LPG). The 5 tons of LPG that were in the tank escaped over two to three hours but fortunately did not catch fire. However, 2,000 people who lived near the plant were evacuated from their homes [11].

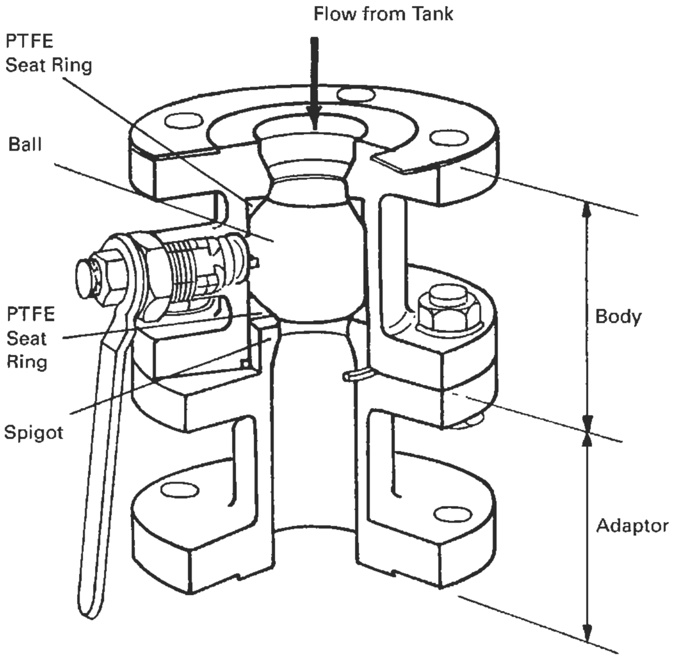


Figure 1-16. Valve dismantled in error.

(c) In canned pumps the moving part of the electric motor—the rotor—is immersed in the process liquid; there is no gland, and gland leaks cannot occur.

The fixed part of the electric motor—the stator—is not immersed in the process liquid and is separated from the rotor by a stainless steel can (Figure 1-17).

If there is a hole in the can, process liquid can get into the stator compartment. A pressure relief plug is therefore fitted to the compartment and should be used before the compartment is opened for work on the stator. Warning plates, reminding us to do this, are often fitted to the pumps.

The stator compartment of a pump was opened up without the pressure relief plug being used. There was a hole in the can. This had caused a pressure buildup in the stator compartment. When the cover was unbolted, it was blown off and hit a scaffold pole 2 m above. On the way up, it hit a man on the knee, and the escaping process vapor caused eye irritation. Persons working on the pump did not know the purpose of the plug, and the warning notice was missing.

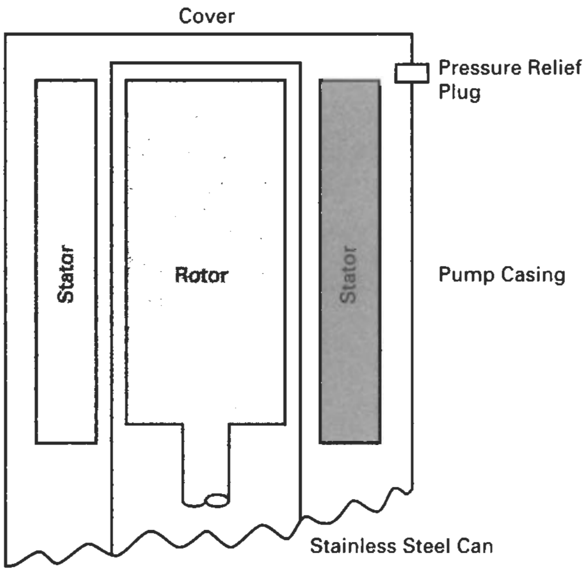


Figure 1-17. Canned pumps.

For a more detailed diagram and description of a canned pump, see Reference 12.

(d) On several occasions, fitters have removed thermowells without realizing that this would result in a leak. They did not realize that the thermowell—the pocket into which a thermocouple or other temperature measuring device sits—is in direct contact with the process fluid. A serious fire that started this way is described in Reference 13.

(e) A high-pressure reciprocating ammonia pump (known as an injector) had run for 23 years without serious problems when the crankshaft suddenly fractured, due to fatigue, and the plungers came out of the cylinders. Two men were killed by the ammonia. No one realized that a failure of the motion work would produce a massive release of ammonia. If people had realized this, they would have installed remotely operated emergency isolation valves (see Section 7.2.1). These would have greatly reduced the size of the leak but would not have acted quickly enough to prevent the fatalities [31].

1.5.5 Treating the Symptoms Instead of the Disease

The following incidents and Section 10.5.3 show what can happen if we go on repairing faults but never ask why so many faults occur.

(a) A cylinder lining on a high-pressure compressor was changed 27 times in nine years. On 11 occasions it was found to be cracked, and on the other 16 occasions it showed signs of wear. No one asked why it had to be changed so often. Everyone just went on changing it. Finally, a bit of the lining got caught between the piston and the cylinder head and split the cylinder.

(b) While a man was unbolting some ¾-in. bolts, one of them sheared. The sudden jerk caused a back strain and absence from work. During the investigation of the accident, seven bolts that had been similarly sheared on previous occasions were found nearby. It was clear that the bolts sheared frequently. If, instead of simply replacing them and carrying on, the workers had reported the failures, then a more suitable bolt material could have been found.

Why did they not report the failures? If they had reported them would anything have been done? The accident would not have occurred if the foreman or the engineer, on their plant tours, had noticed the broken bolts and asked why there were so many.

(c) A line frequently choked. As a result of attempts to clear the chokes, the line was hammered almost flat in several places. It would have been better to have replaced the line with a larger one or with a line that had a greater fall, more gentle bends, or rodding points.

1.5.6 Flameproof Electrical Equipment

On many occasions, detailed inspections of flameproof electrical equipment have shown that many items were faulty. For example, at one plant a first look around indicated that nothing much was wrong. A more thorough inspection, paying particular attention to equipment not readily accessible and that could be examined only from a ladder, showed that out of 121 items examined, 33 needed repair. The faults included missing and loose screws, gaps too large, broken glasses, and incorrect glands. Not all the faults would have made the equipment a source of ignition, but many would have done so.

Why were there so many faults? Before this inspection, there had been no regular inspections. Many electricians did not understand why flameproof equipment was used and what would happen if it was badly maintained. Spare screws and screwdrivers of the special types used were not in stock, so there was no way of replacing those lost.

Regular inspections were set up. Electricians were trained in the reasons why flameproof equipment is used, and spares were stocked. In addition, it was found that in many cases flameproof equipment was not really necessary. Division (Zone) 2 equipment—cheaper to buy and easier to maintain—could be used instead.

1.5.7 Botching

Section 1.5.3 (a) described a botched job. Here are two more.

(a) A pressure vessel was fitted with a quick-opening lid, 10 in. diameter, secured by four eye-bolts (Figure 1-18). They had to be replaced, as the threads were corroded. Instead of replacing the whole eye-bolt, a well-meaning person decided to save time by simply cutting the eyes off the bolts and welding new studs onto them. As soon as the vessel was pressurized (with compressed air) the new studs, which had been made brittle by the welding, failed, and the lid flew off. Fortunately a short length of chain restrained it, and it did not fly very far [38]. (See Sections 13.5 and 17.1 for the hazards of quick-opening lids.)

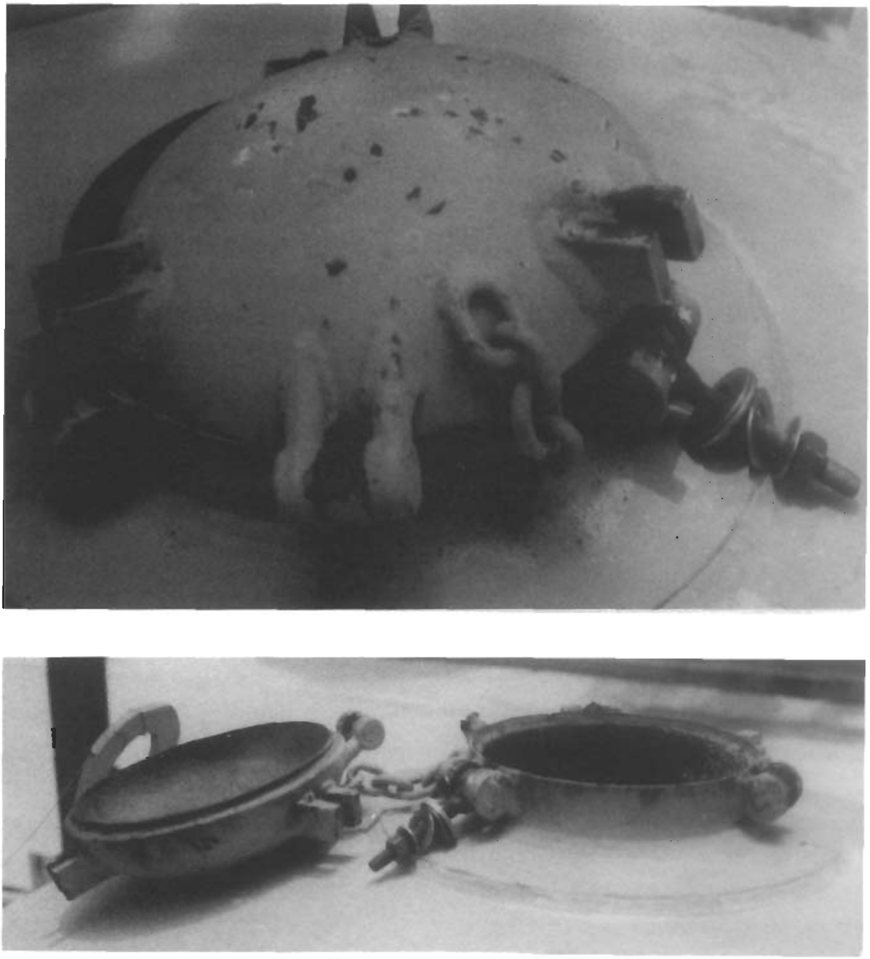


Figure 1-18. Instead of replacing the eye-bolts, new studs were welded in place of the threaded portions. They were made brittle by the heat and failed in use. Fortunately the chain prevented the lid from going into orbit.

(b) A screwdriver was left in the steering column of a truck after the truck was serviced. The truck and semitrailer crashed, and the servicing company had to pay $250,000 in damages. To quote from the report, "Workplaces need to be as rigorous as the aviation and medical industries in ensuring that all tools are accounted for when servicing is completed" [39].

1.5.8 Who Should Decide How to Carry Out a Repair?

The following report raises two interesting questions:

- Who decides how a maintenance job should be carried out?
- How should we clear chokes in small bore lines?

A sample point on the suction line of two water pumps became choked, and a maintenance worker was asked to clear it. He was not told how to do so—craftsmen dislike people from other departments telling them how to do their jobs—but the operators assumed he would use water under pressure or a rod. Instead he used compressed air at a gauge pressure of 115 psi (8 bar), and a pocket of air caused the pumps to lose suction (Figure 1-19).

The results were not serious. The pumps supplied water to cool the hot gases leaving an incinerator; when the water flow stopped, a high-temperature trip shut down the burner. The incinerator was new, was still undergoing tests, and the job had not been done before. The water was recycled, and ash in it probably caused the choke [40].

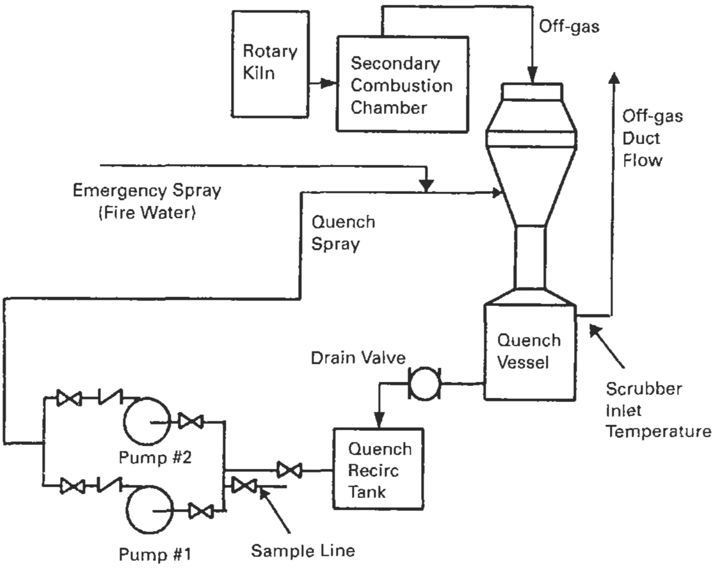


Figure 1-19. Simplified drawing of incinerator quench recirculation system. *(Illustration courtesy of the U.S. Department of Energy.)*

According to the report, the maintenance worker should have been given more detailed instructions. But, as it also points out, some skills are skills of the craft; we should be able to assume that craftsmen are aware of them and should not need to give them detailed instructions on each and every occasion. We should not need to tell them, for example, how to break a joint every time they are asked to do so (but see Section 1.5.1). Where do we draw the line?

Craftsmen (and operators) ought to be taught, as part of their safety training, that compressed gases should not be used to clear chokes. There is a lot of energy in a compressed gas, and it can accelerate a plug to great speed, putting it into orbit if there is an open end or breaking a pipeline if the plug hits a bend (see Section 17.2).

This incident shows how much we can learn from a simple event if we treat it as a learning experience and do not say, "No one was hurt, and there was no damage, so let's forget about it."

1.6 A PERSONAL NOTE

The recommendations described in this Chapter go further than some companies consider necessary. For example, companies may put Do Not Operate notices on valves instead of locks, or to save time, they may turn a blind eye to occasional shortcuts. Nevertheless, bitter experience has convinced me that the recommendations are necessary.

In 1968, after 16 of years experience in production, I was transferred to a new position in safety. It was an unusual move at the time for someone with my background, but five deaths from three serious fires in three years, two of them the results of poor preparation for maintenance, convinced the senior management that more resources should be devoted to safety and that it could no longer be left to nontechnical people and elderly foremen. Since then I have read scores of reports about other accidents that happened because of this cause. Some were serious; others were near-misses.

When I retired from industry one of my first tasks was to sort the many accident reports I had collected. The thickest folder by far was one labeled Preparation For Maintenance. Some of the incidents from that folder, together with more recent ones, are described above.

If you decide my recommendations are not right for your organization, please do not ignore the accidents I have described. Check that your procedures will prevent them, or they will happen again.

REFERENCES

1. T. A. Kletz, in D. A. Crowl and S. S. Grossel (editors), *Handbook of Toxic Materials Handling and Management,* Marcel-Dekker, New York, 1994, Chapter 11.
2. F. P. Lees, *Loss Prevention in the Process Industries,* 2nd edition, Butterworth-Heinemann, Oxford, UK, Chapter 21.
3. T. A. Kletz, *Lessons From Disaster: How Organizations Have No Memory and Accidents Recur,* co-published by Institution of Chemical Engineers, Rugby, UK, and Gulf Publishing Co., Houston, Texas, 1993.
4. *Annual Report of the Chief Inspector of Factories for 1974,* Her Majesty's Stationery Office, London, 1975, p. 19.
5. *The Bulletin, The Journal of the Society for Petroleum Acts Administration,* Oct. 1970, p. 68.
6. *Chemical Safety Summary,* Chemical Industries Association, London, July–Sept. 1980, p. 15.
7. *Petroleum Review,* Apr. 1982, p. 34.
8. *Annual Report of Her Majesty's Inspectors of Explosives for 1970,* Her Majesty's Stationery Office, London, 1971, p. 19.
9. *Health and Safety—Manufacturing and Service Industries 1979,* Her Majesty's Stationery Office, London, 1981, p. 62.
10. T. A. Kletz, *Hydrocarbon Processing,* Vol. 61, No. 3, Mar. 1982, p. 207.
11. Health and Safety Executive, *Leakage of Propane at Whitefriars Glass Limited, Wealdstone, Middlesex, 20 November 1980,* Her Majesty's Stationery Office, London, 1981.
12. G. R. Webster, *The Chemical Engineer,* Feb. 1979, p. 91.
13. *Petroleum Review,* Oct. 1981, p. 21.
14. J. H. Christiansen and L. E. Jørgensen, *Proceedings of the Fourth International Symposium on Loss Prevention and Safety Promotion in the Process Industries* (Symposium held in Harrogate, UK, Sept. 1983), Institution of Chemical Engineers, Rugby, UK, p. L9.
15. L. G. Britton and J. A. Smith, *Plant/Operations Progress,* Vol. 7, No. 1, Jan. 1988, p. 53.

16. *The Phillips 66 Company Houston Chemical Complex Explosion and Fire,* U.S. Dept. of Labor, Washington, D.C., Apr. 1990.
17. *Oil and Gas Journal,* May 28, 1990, p. 36.
18. W. D. Cullen, *The Public Inquiry into the Piper Alpha Disaster,* Her Majesty's Stationery Office, London, 1990, especially Paragraphs 6.109, 6.187, 11.3, and 18.29.
19. *Loss Prevention Bulletin,* No. 091, Feb. 1990, p. 17.
20. *Potential Fire Hazard from Anaerobic Decomposition in Cooling Water System,* Safety Note No. DOE/EH-0109, U.S. Dept. of Energy, Washington, D.C., Oct. 1989.
21. H. E. Watts, *Report on Explosion in Kerosene Tank at Killingholme, Lincs.,* Her Majesty's Stationery Office, London, 1938.
22. *Loss Prevention Bulletin,* No. 099, Apr. 1991, p. 9.
23. C. H. Vervalin, *Hydrocarbon Processing,* Vol. 51, No. 12, Dec. 1972, p. 52.
24. *Loss Prevention Bulletin,* No. 098, Apr. 1991, p. 25.
25. *Labeling Errors Cause Accidents,* Safety Note No. DOE/EH-0328, U.S. Dept. of Energy, Washington, D.C., July 1993.
26. C. W. Ramsay, *Plant/Operations Progress,* Vol. 9, No. 2, Apr. 1990, p. 117.
27. *Occupational Health and Safety Observer,* Vol. 2, No. 6, U.S. Dept. of Energy, Washington, D.C., June 1993, p. 6.
28. B. A. Prine, "Analysis of Titanium/Carbon Steel Heat Exchanger Fire," Paper presented at AIChE Loss Prevention Symposium, Aug. 1991.
29. *Occupational Health and Safety Observer,* Vol. 2, No. 1, U.S. Dept of Energy, Washington, D.C., Sept. 1993, p. 3.
30. *Loss Prevention Bulletin,* No. 100, Aug. 1991, p. 35.
31. P. J. Nightingale, "Major Incident Following the Failure of an Ammonia Injector on a Urea Plant," Paper presented at AIChE Ammonia Symposium, Aug. 1990.
32. *Operating Experience Weekly Summary,* No. 96-50, Office of Nuclear and Facility Safety, U.S. Dept. of Energy, Washington, D.C., 1996, p. 9.
33. *Loss Prevention Bulletin,* No. 107, Oct. 1992, p. 17.

34. *Operating Experience Weekly Summary,* No. 96-44, Office of Nuclear and Facility Safety, U.S. Dept. of Energy, Washington, D.C., 1996, p. 2.

35. *Occupational Safety and Health Observer,* Vol. 3, Nos. 7 and 8, U.S. Dept. of Energy, Washington, D.C., July–Aug. 1994, p. 1.

36. *Underground Utilities Detection and Excavation,* Safety Notice No. DOE/EH-0541, Office of Nuclear and Facility Safety, U.S. Dept. of Energy, Washington, D.C., 1996.

37. *Effective Shift Handover—A Literature Review,* Report No. OTO 96 003, Health and Safety Executive, Sheffield, UK, 1996, p. 7.

38. R. E. Sanders and W. L. Spier, *Process Safety Progress,* Vol. 15, No. 4, Winter 1996, p. 189.

39. *Safety Management,* South Africa, Sept. 1995, p. 2. Though reported in a South African magazine, the incident occurred in Australia.

40. *Operating Experience Weekly Summary,* Nos. 96-46 and 96-49, Office of Nuclear and Safety Facility, U.S. Dept. of Energy, Washington, D.C., 1996, pp. 9 (of 96-46) and 2 (of 96-49).

41. *Operating Experience Weekly Summary,* No. 97-20, Office of Nuclear and Facility Safety, U.S. Dept. of Energy, Washington, D.C., 1997, p. 2.

42. *Operating Experience Weekly Summary,* No. 97-15, Office of Nuclear and Facility Safety, U.S. Dept. of Energy, Washington, D.C., 1997, p. 7.

43. J. A. Senecal, *Journal of Loss Prevention in the Process Industries,* Vol. 4, No. 5, 1991, p. 332.

44. *Operating Experience Weekly Summary,* No. 97-22, Office of Nuclear and Facility Safety, U.S. Dept. of Energy, Washington, D.C., 1997, p. 3.

45. *Loss Prevention Bulletin,* No. 098, Apr. 1991, p. 25.

46. Health and Safety Executive, *Dangerous Maintenance,* Her Majesty's Stationery Office, London, 1987, p. 8.

Chapter 2

Modifications

> I consider it right that every talented man should be at liberty to make improvements, but that the supposed improvements should be duly considered by proper judges.
>
> —George Stephenson, 1841

Many accidents have occurred because changes were made in plants or processes and these changes had unforeseen side effects. In this chapter a number of such incidents are described. How to prevent similar changes in the future is discussed. Some of the incidents are taken from References 1 and 2, where others are described as well.

2.1 STARTUP MODIFICATIONS

Startup is a time when many modifications may have to be made. It is always a time of intense pressure. It is therefore not surprising that some modifications introduced during startup have had serious unforeseen consequences.

At one plant, a repeat relief and blowdown review was carried out one year after startup. The startup team had been well aware of the need to look for the consequences of modifications and had tried to do so as modifications were made. Nevertheless, the repeat relief and blowdown review brought to light 12 instances in which the assumptions of the original review were no longer true and additional or larger relief valves, or changes in the position of a relief valve, were necessary. Figure 2-1 shows some examples.

The line diagrams had been kept up-to-date despite the pressures on the plant staff during startup. This made it easier to repeat the relief and blowdown review. The plant staff members were so impressed by the results that they decided to have another look at the relief and blowdown after another year.

Section 5.5.2 (c) describes a late change in design that had unforeseen results.

2.2 MINOR MODIFICATIONS

This term is used to describe modifications so inexpensive that they either do not require formal financial sanction or the sanction is easily

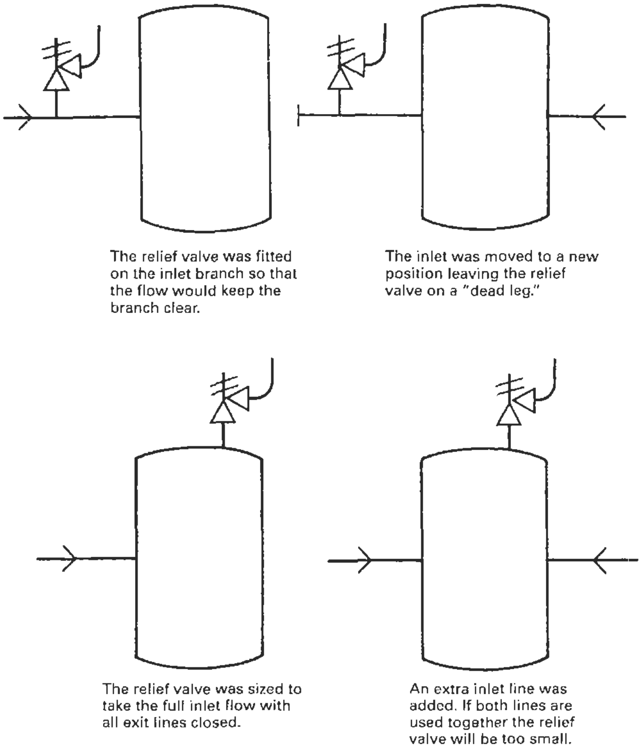


Figure 2-1. Some of the modifications made to the relief system in a plant during its first year on line.

(figure continued on next page)

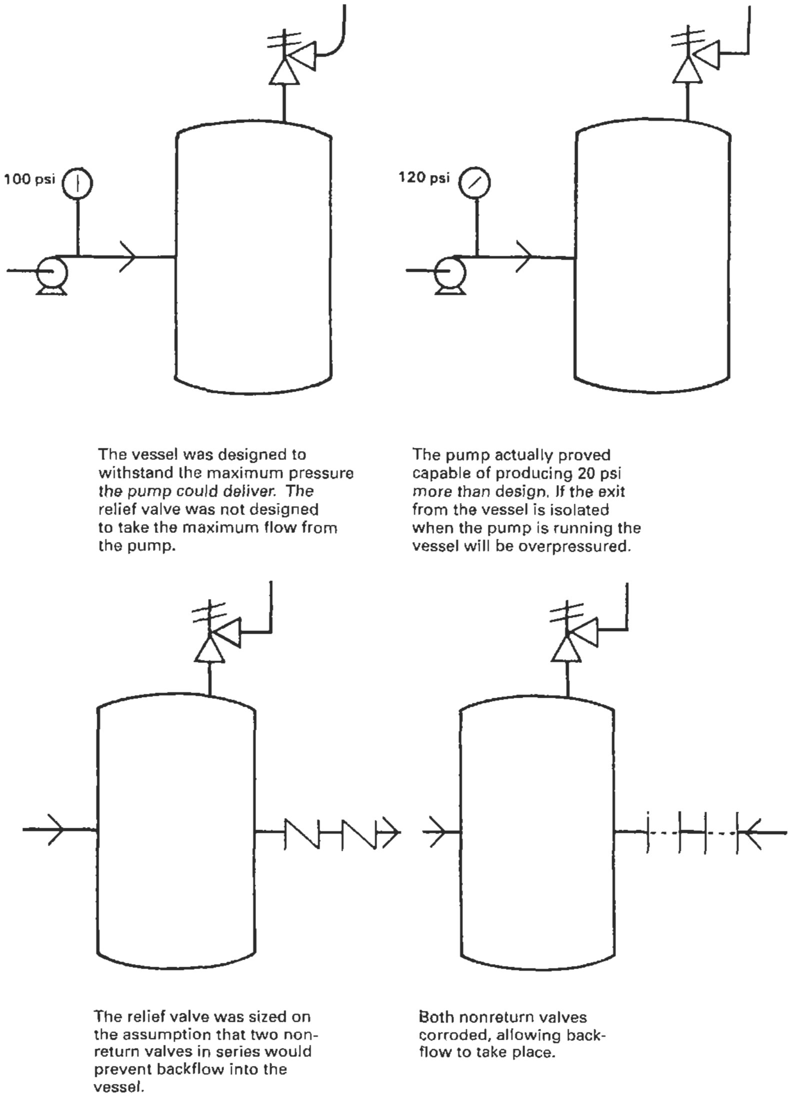


Figure 2-1. Continued.

obtained. They therefore may not receive the same detailed consideration as a more expensive modification.

(a) A modification so simple that it required only a work permit resulted in the end blowing off a tank and fatal injuries to two men working in the area.

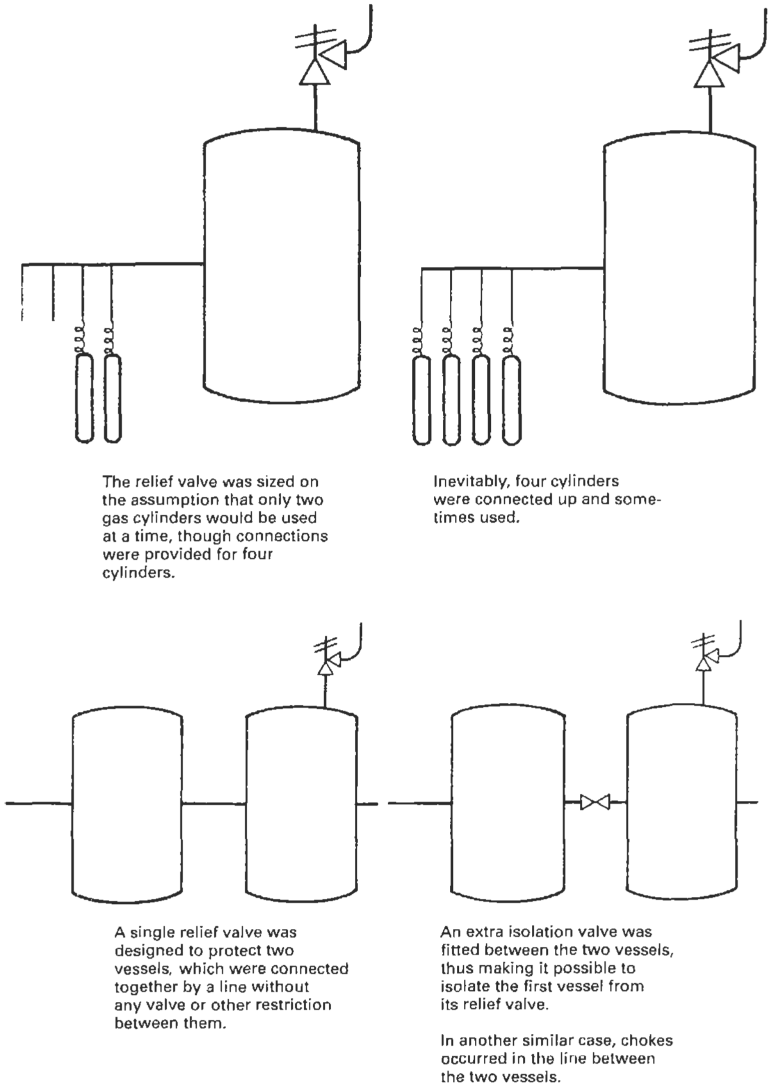


Figure 2-1. Continued.

The tank was used for storing a liquid product that melts at 97°C. It was therefore heated by a steam coil using steam at a gauge pressure of 100 psi (7 bar). At the time of the incident, the tank was almost empty and was being prepared to receive some product. The inlet line was being blown with compressed air to prove that it was clear—the normal procedure before filling the

tank. The air was not getting through, and the operator suspected a choke in the pipeline.

In fact, the vent on the tank was choked. The gauge air pressure (75 psi or 5 bar) was sufficient to burst the tank (design gauge pressure 5 psi or 0.3 bar). Originally the tank had a 6-in.-diameter vent. But at some time this was blanked off, and a 3-in.-diameter dip branch was used instead as the vent.

Several other things were wrong. The vent was not heated; its location made it difficult to inspect. Most important of all, neither manager, supervisors, nor operators recognized that if the vent choked, the air pressure was sufficient to burst the tank. Nevertheless, if the 6-in. vent had not been blanked, the incident would not have occurred (see also Section 12.1).

(b) A reactor was fitted with a bypass (Figure 2-2a). The remotely operated valves A, B, and C were interlocked so that C had to be open before A or B could be closed. It was found that the valves leaked, so hand-operated isolation valves (a, b and c) were installed in series with them (Figure 2-2b).

After closing A and B, the operators were instructed to go outside and close the corresponding hand valves a and b. This destroyed the interlocking. One day an operator could not get A and B to close. He had forgotten to open C. He decided that A and B were faulty and closed a and b. Flow stopped. The tubes in the furnace were overheated. One of them burst, and the lives of the rest were shortened.

(c) A let-down valve was a bottleneck, so a second let-down valve was added in parallel (Figure 2-3). During installation, the check valve was hidden beneath insulation and was not noticed, and the parallel line was joined to the original line downstream of the check valve where there was a convenient branch. The upstream equipment was thus connected directly to the downstream equipment, bypassing the relief valve.

A blockage occurred downstream. The new let-down valve was leaking, and the downstream equipment was overpressured and burst.

When the modification was designed, the designers assumed that the new line would join the original line immediately after the relief valve. If they realized the importance of this, they did not

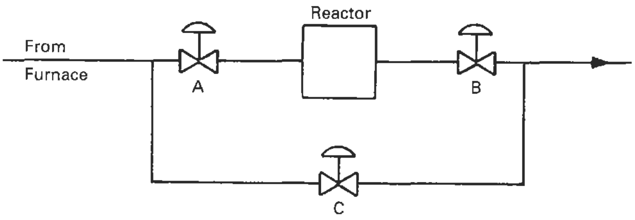


Figure 2-2a. Original reactor bypass.

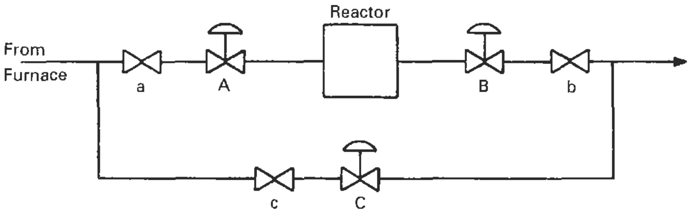


Figure 2-2b. Modified reactor bypass.

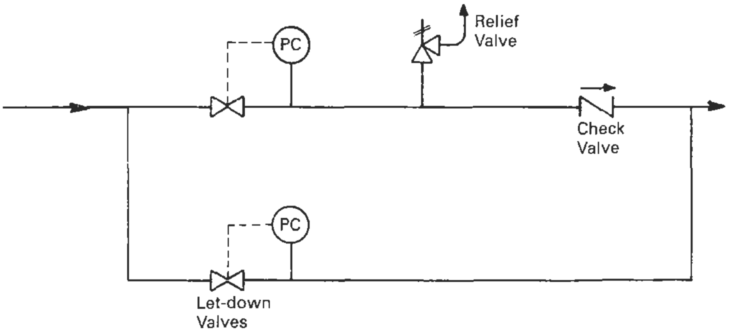


Figure 2-3. The second (lower) let-down valve was joined to the original line downstream of the check valve. When this let-down valve leaked, the downstream equipment was overpressured.

draw attention to it, and they did not check that the modification had been made correctly [13].

Modifications should always be marked on a line diagram before they are approved, and the person who authorizes them should always inspect the finished modification to make sure that his or her intentions have been followed.

(d) A group of three rooms in a control center were pressurized to prevent the entry of hazardous vapors. A fan blew air into room 1, and it passed through louvers into room 2 and from there into room 3. A pressure controller measured the pressure in room 1. For an unknown reason, the louvers between rooms 1 and 2 were blocked. Six years passed before anyone realized that the pressures in the other rooms were not under control [20]. The company had a procedure for the control of modifications, but it was not used when the louvers were blocked, perhaps because those concerned thought it applied only to plant equipment and not to buildings. What would happen on your plant?

In another building, gusting winds caused transient increases in pressure that tripped the ventilation fans. The problem was overcome by increasing the fan speeds. Unfortunately the increased flow of cold air through a doorway cooled a fire water main so much that it froze and cracked [21].

(e) Other minor modifications that have had serious effects on plant safety are:

1. Removing a restriction plate that limits the flow into a vessel and that has been taken into account when sizing the vessel's relief valve. A length of narrow bore pipe is safer than a restriction plate, as it is less easily removed.
2. Fitting a larger trim into a control valve when the size of the trim limits the flow into a vessel and has been taken into account when sizing the vessel's relief valve.
3. Fitting a substandard drain valve (see Section 8.2 a).
4. Replacing a metal duct or pipe by a hose (see Section 15.3.)
5. Solid was scraped off a flaker—a rotating steel drum—by a steel knife. After the knife was replaced by a plastic one, an explosion occurred, probably because more dust was produced [14].
6. Without consulting the manufacturer, the owner of a set of hot tapping equipment made a small modification: he installed a larger vent valve to speed up its use. As a result the equipment could no longer withstand the pressure and was violently ejected from a pipeline operating at a gauge pressure of 40 bar (600 psi) [22].
7. Making a small change in the size of a valve spindle and thus changing its natural frequency of vibration (see Section 9.1.2 a).
8. Changing the level in a vessel (see Sections 2.6 i, 22.2 d and e).

2.3 MODIFICATIONS MADE DURING MAINTENANCE

Even when systems for controlling modifications have been set up, modifications often slip in unchecked during maintenance. (Someone decides, for what he or she thinks is a good reason, to make a slight change.)

Many years ago a special network of air lines was installed for use with air masks only. A special branch was taken off the top of the compressed air main as it entered the works (Figure 2-4).

For 30 years this system was used without any complaint. Then one day a man got a faceful of water while wearing an air mask inside a vessel. Fortunately he was able to signal to the stand-by man that something was wrong, and he was rescued before he suffered any harm.

Investigation found that the compressed air main had been renewed and that the branch to the breathing apparatus network had been moved to the *bottom* of the main. When a slug of water got into the main, it all went into the catchpot, which filled up more quickly than it could empty. Unfortunately, everyone had forgotten why the branch came off the top of the main, and nobody realized that this was important.

A very similar incident occurred on a fuel-gas system. When a corroded main was renewed, a branch to a furnace was taken off the bottom of the main instead of the top. A slug of liquid filled up the catchpot and extinguished the burners.

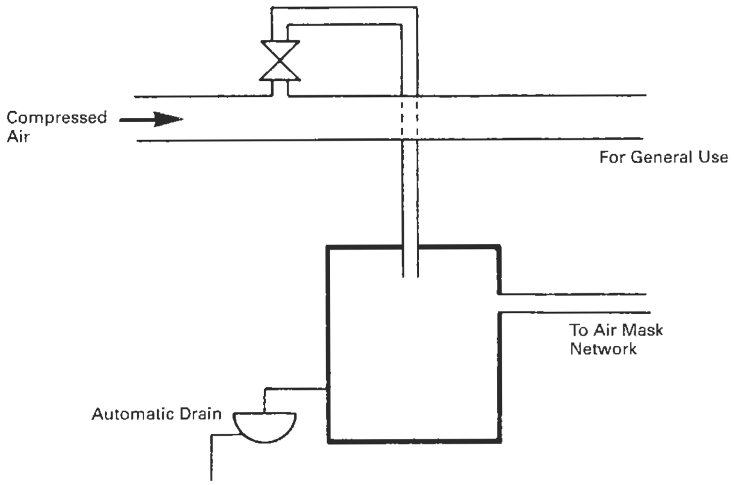


Figure 2-4. Original arrangement of air lines.

Some hot (370°C) pipework was supported by spring hangers to minimize stress as it was heated and cooled. The atmosphere was corrosive, and the spring hangers became impaired. They were removed, and the pipework was left solidly supported. It could not withstand the stress, and a condenser fractured; hot heat-transfer oil was released and caught fire.

No one, it seems, realized the importance of the supports. Unlike the pipework, they were not protected against corrosion and were removed with little or no thought about the consequences [23].

As the result of some problems with a compressor, changes were made to the design of a shaft labyrinth. A new one was ordered and installed, but a spare of the old design was left in the store. Eight years later, after the staff had changed, the part had to be replaced. You've guessed what happened: the old spare was withdrawn from the store and installed.

A similar incident occurred on a boiler. After the No. 1 roof tube had failed several times, it was replaced by a thicker tube, and the change marked on the drawings. Some time later a small leak developed in this tube, and a length had to be replaced. No one looked at the drawings, and a 0.5 m length of standard tube was welded in. The discontinuity caused turbulence, local overheating, and rapid failure [24].

Moving people is a modification of which the consequences are rarely considered.

2.4 TEMPORARY MODIFICATIONS

(a) The most famous of all temporary modifications is the temporary pipe installed in the Nypro Factory at Flixborough, UK, in 1974. It failed two months later, causing the release of about 50 tons of hot cyclohexane. The cyclohexane mixed with the air and exploded, killing 28 people and destroying the plant [3, 25, 26].

At the Flixborough plant there were six reactors in series. Each reactor was slightly lower than the one before so that the liquid in them flowed by gravity from No. 1 down to No. 6 through short 28-in.-diameter connecting pipes (Figure 2-5). To allow for expansion, each 28-in. pipe contained a bellows (expansion joint).

One of the reactors developed a crack and had to be removed. (The crack was the result of a process modification; see Section 2.6 b.) It was replaced by a temporary 20-in. pipe, which had two bends in it, to allow for the difference in height. The existing bellows were left in position at both ends of the temporary pipe (Figure 2-5).

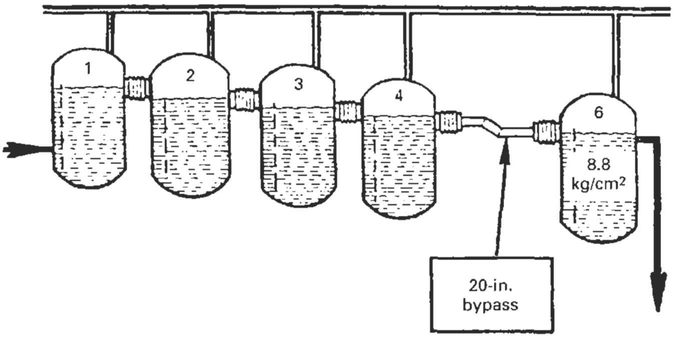


Figure 2-5. Arrangement of reactors and temporary pipe at Flixborough.

The design of the pipe and support left much to be desired. The pipe was not properly supported: it merely rested on scaffolding. Because there was a bellows at each end, it was free to rotate or "squirm" and did so when the pressure rose a little above the normal level. This caused the bellows to fail.

No professionally qualified engineer was in the plant at the time the temporary pipe was built. The men who designed and built it (*design* is hardly the word because the only drawing was a full-scale sketch in chalk on the workshop floor) did not know how to design large pipes required to operate at high temperatures (150°C) and gauge pressures (150 psi or 10 bar). Very few engineers have the specialized knowledge to design highly stressed piping. But in addition, the engineers at Flixborough did not know that design by experts was necessary.

They did not know what they did not know [25, 26].

(b) A reactor was cooled by a supply of brine to the jacket. The brine system had to be shut down for repair, so town water was used instead. The pressure of the town water (a gauge pressure of 130 psi or 9 bar) was higher than that of the brine, and the reactor collapsed.

A modification approval form, containing 20 questions, had been completed before the modification was made but this was treated as a formality, and the questions were answered in a perfunctory manner [6].

For another temporary modification see Section 5.5.1.

2.5 SANCTIONED MODIFICATIONS

This term is used to describe modifications for which the money has to be authorized by a senior manager or a committee. They cannot, therefore, be done in a hurry. Justifications have to be written out and people persuaded. Although the systems are (or have been in the past) designed primarily to control cost rather than safety, they usually result in careful consideration of the proposal by technical personnel. Unforeseen consequences may come to mind, though not always. Sometimes sanction is obtained before detailed design has been carried out, and the design may then escape detailed considerations. Nevertheless, it is harder to find examples of serious incidents caused by sanctioned modifications. The following might almost rank as a startup modification. Though the change was agreed upon more than a year before startup, it occurred after the initial design had been studied and approved.

(a) A low-pressure refrigerated ethylene tank was provided with a relief valve set at a gauge pressure of about 1.5 psi (0.1 bar), which discharged to a vent stack. After the design had been completed, it was realized that cold gas coming out of the stack would, when the wind speed was low, drift down to ground level, where it might be ignited. The stack was too low to be used as a flarestack—the radiation at ground level would be too high—and was not strong enough to be extended. What could be done?

Someone suggested putting steam up the stack to disperse the cold vapor. This seemed a good idea and the suggestion was adopted (Figure 2-6).

As the cold vapor flowed up the stack, it met condensate flowing down. The condensate froze and completely blocked the 8-in.-diameter stack. The tank was overpressured and ruptured. Fortunately, the rupture was a small one and the escaping ethylene did not ignite. It was dispersed with steam while the tank was emptied.

Should the design team have foreseen that the condensate might freeze? A hazard and operability study (see Chapter 18) would probably have drawn attention to the hazard.

After the tank was repaired, the vent stack was replaced by a flarestack.

(See also Sections 3.3.1 b, 6.2 b, 8.1.6, and 9.2.1 g.)

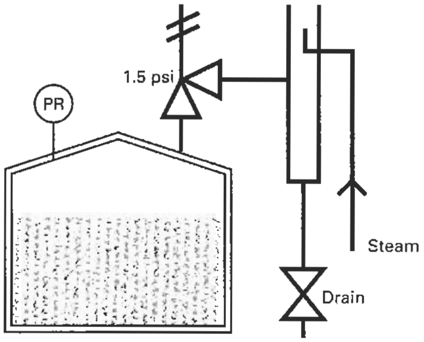


Figure 2-6. Liquid ethylene tank venting arrangements.

(b) A new loading gantry was built for filling tank trucks with liquefied petroleum gas. The ground was sloped so that any spillages would run away from the tanker and would not heat it if they caught fire. As a result of this change in design, it was found that the level indicator would not read correctly when the tank truck was located on sloping ground. The design had to be modified again so that the wheels stood on level ground, but the ground in between and around them was sloped.

(c) A "carbon copy" plant was built with the floors 3 m (10 ft) apart instead of 2.4 m (8 ft) apart, as 3 m was the company standard. The increased height was too much for convection flow, and efficiency was lost.

(d) When construction of a nuclear power station was well under way, an advisory committee suggested that a zirconium liner should be added to part of the cooling circuit. The operating company did not think the liner was necessary, but it was cheap to install; proving that it was unncessary would have cost more than installing the liner, so the company installed it. Bits of it came loose and blocked the cooling circuit; the reactor overheated and was damaged, but there was no release of radioactivity. The liner was not replaced when the reactor was repaired [15].

The operator of a plant, not an advisory committee, however eminent, is responsible for the safety of the plant and should not follow advice that it believes to be wrong just to save costs or avoid arguments.

Another sanctioned modification is described in Section 12.4.6.

2.6 PROCESS MODIFICATIONS

So far we have discussed modifications to the plant equipment. Accidents can also occur because changes to process materials or conditions had unforeseen results, as the following cases and Section 19.5 show:

(a) A hydrogenation reactor developed a pressure drop. Various causes were considered—catalyst quality, size, distribution, activation, reactant quality, distribution and degradation—before the true cause was found.

The hydrogen came from another plant and was passed through a charcoal filter to remove traces of oil before it left the supplying plant. Changes of charcoal were infrequent, and the initial stock lasted several years. Reordering resulted in a finer charcoal being supplied and charged without the significance of the change being recognized. Over a long period, the new charcoal passed through its support into the line to the other plant. Small amounts of the charcoal partially clogged the ⅜-in. distribution holes in the catalyst retaining plate (Figure 2-7). There was a big loss of production.

The cause of the pressure drop was difficult to find because it was due to a change in another plant.

(b) At one time, it was common to pour water over equipment that was too hot or that was leaking fumes. The water was taken from the

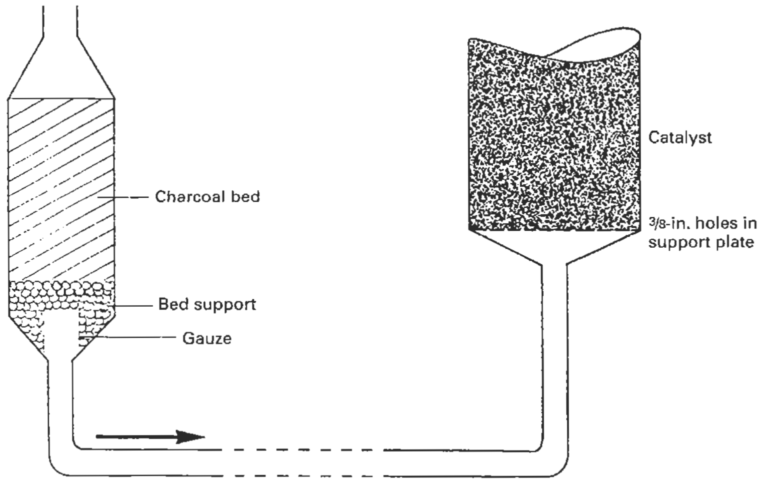


Figure 2-7. Hydrogen purification system.

nearest convenient supply. At Flixborough, there was a leak of cyclohexane vapor from the stirrer gland on one of the reactors. To condense the leaking vapor, water was poured over the top of the reactor. Plant cooling water was used because it was conveniently available.

Unfortunately, the water contained nitrates, which caused stress corrosion cracking of the mild steel reactor. The reactor was removed for repair, and the temporary pipe that replaced it later failed and caused the explosion (see Section 2.4).

Nitrate-induced cracking is well known to metallurgists but was not well known to other engineers at the time. Before you poured water over equipment—emergencies apart—would you ask what the water contained and what its effect would be on the equipment?

Pouring water over equipment is a change from normal operating practice. It should therefore be treated as a modification. For a description of nitrate cracking of mild steel, see Reference 4.

(c) The following incident shows how difficult it is to foresee all the results of a change and how effects can be produced a long way downstream of the place where the change is made:

Some radioactive bromine (half-life 36 hours), in the form of ammonium bromide, was put into a brine stream as a radioactive tracer. At another plant 30 km away, the brine stream was electrolyzed to produce chlorine. Radioactive bromine entered the chlorine stream and subsequently concentrated in the base of a distillation column, which removed heavy ends. This column was fitted with a radioactive-level controller. The radioactive bromine affected the level controller, which registered a low level and closed the bottom valve on the column. The column became flooded. There was no injury, but production was interrupted.

(d) A minor change in operating conditions can sometimes have devastating results. A nitration reaction was carried out at low temperature, and then the reactor was heated to 90°C and kept at this temperature for 30 minutes; it was then cooled. After a year's operation, someone decided to let the batch cool by heat loss to the surroundings with no one in attendance, as soon as the temperature reached 90°C. An explosion occurred; the building was wrecked, and parts of the reactor were found 75 m away [7].

(e) The heating in a building had to be shut down over a weekend for repairs. There were fears that the water in the sprinkler system might freeze, so it was replaced by alcohol. A fire occurred and was fed by the sprinklers!

(f) Aqueous ammonia was added to a plant to reduce corrosion. The corrosion stopped, but the liquid droplets caused erosion, a pipe failure, and a substantial fire [8].

(g) Three vacuum stills were fitted with steam ejectors and direct contact condensers. The water was cooled in a small cooling tower and recycled, and the small amount of vapor carried over from the stills dispersed in the tower. The tower was fitted with a fan, but to save electricity, the operators switched off the fan and found that they could get adequate cooling without it. However, the flammable vapors from the stills were no longer dispersed so effectively. This was discovered when an operator, about to light a furnace a few meters away, tested the atmosphere inside the furnace in the usual way—with a combustible gas detector—and found that gas was present.

No one realized, when a site for the furnace was decided, that flammable vapors could come out of the cooling tower. Direct contact condensers are not common, but flammable vapors can appear in many cooling towers if there are leaks on water-cooled heat exchangers. After the incident, a combustible gas detector was mounted permanently between the furnace and the tower (Figure 2-8).

(h) To meet new Environmental Protection Agency requirements, the fuel oil used for two emergency diesel generators was changed to a low-sulfur grade (from 0.3% maximum to 0.05% maximum). The lubricating oil used contained an additive that neutralized the sulfuric acid formed during combustion. With less acid produced, the excess additive formed carbon deposits, which built up behind the piston rings, causing them to damage the cylinder walls. Fortunately the problem was found after test runs and solved by changing the type of lubricating oil, before the generators were needed in an emergency [27].

(i) A sparger was removed for inspection and found to be corroded, though it had been in use for 30 years and never been known to corrode before. The problem was traced to a change in the level in the vessel so that the sparger was repeatedly wetted and then dried [28].

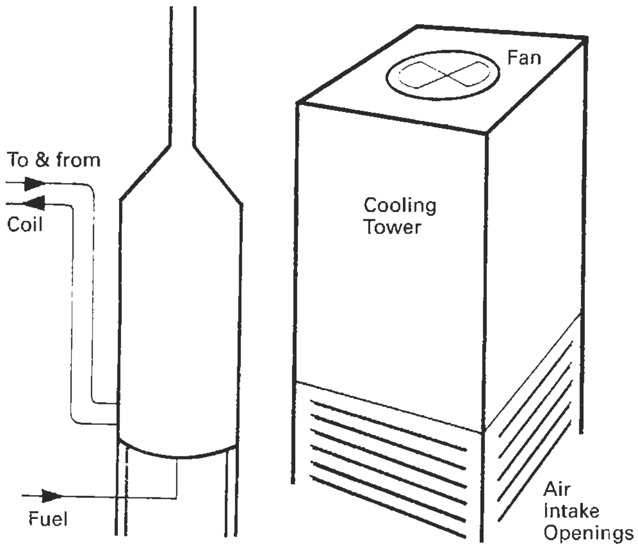


Figure 2-8. Gas entered the furnace when the cooling tower fan was switched off.

(j) The storage tank on a small detergent bottling plant was washed out every week. A small amount of dilute washings was allowed to flow into the dike and from there to drain. The operators carrying out the washing had to work in the dike and got their feet wet. so they connected a hose to the drain valve, put the other end into the sewer, and left it there. You've guessed right again. After a few months someone left the drain valve open. When the tank was filled, 20 m^3 of detergent went down the drain. It overloaded the sewage plant. and a 3-m-high wall of foam moved down the local river [29].

(k) The duckpond at a company guesthouse was full of weeds, so the company water chemist was asked for advice. He added an herbicide to the pond. It was also a detergent; it wetted the ducks' feathers, and the ducks sank.

2.7 NEW TOOLS

The introduction of new tools can have unforeseen side effects:

(a) On several occasions, radioactive level indicators have been affected by radiography being carried out on welds up to 70 m away.

(b) This incident did not occur in the process industries, but nevertheless is a good example of the way a new tool can introduce unforeseen hazards:

A natural gas company employed a contractor to install a 2-in. plastic natural gas main to operate at a gauge pressure of 60 psi (4 bar) along a street. The contractor used a pneumatic boring technique. In doing so, he bored right through a 6-in. sewer pipe serving one of the houses on the street.

The occupant of the house, finding that his sewer was obstructed, engaged another contractor to clear it. The contractor used an auger and ruptured the plastic gas pipe. Within three minutes, the natural gas had traveled 12 m up the sewer pipe into the house and exploded. Two people were killed and four injured. The house was destroyed, and the houses on both sides were damaged.

After the explosion, it was found that the gas main had passed through a number of other sewer pipes [5].

2.8 ORGANIZATIONAL CHANGES

These can also have unforeseen side effects, as shown by the following incidents:

(a) A plant used sulfuric acid and caustic soda in small quantities, so the two substances were supplied in similar plastic containers called polycrates (Figure 2-9). While an operator was on his day off, someone decided it would be more convenient to have a polycrate of acid and a polycrate of alkali on each side (Figure 2-10). When the operator came back, no one told him about the change. Without checking the labels, he poured some excess acid into a caustic crate. There was a violent reaction, and the operator was sprayed in the face. Fortunately he was wearing goggles.

We should tell people about changes made while they were away. In addition, if incompatible chemicals are handled at the same plant, then, whenever possible, the containers should differ in size, shape, and/or color, and the labels should be large and easily seen from eye level.

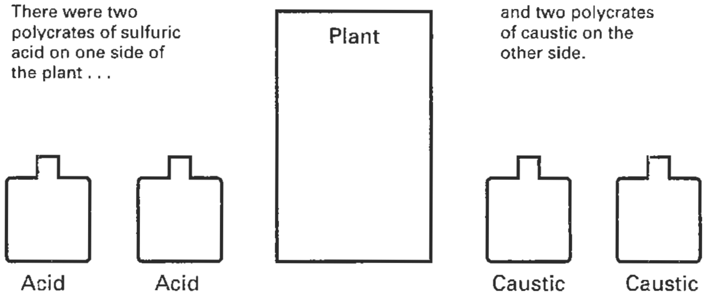


Figure 2-9. Original layout of acid and caustic containers.

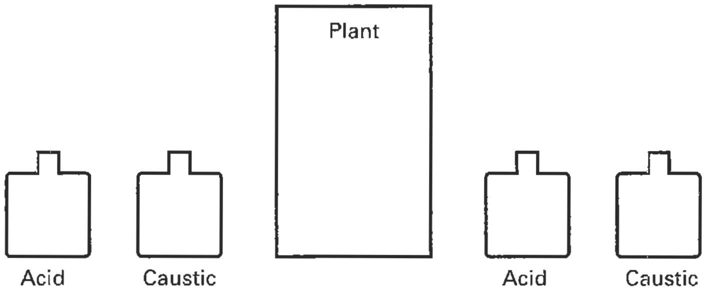


Figure 2-10. Modified layout of acid and caustic containers.

(b) The staff of a plant decided to exhibit work permits so that they could be more readily seen by workers on the job—a good idea.

The permits were usually put in plastic bags and tied to the equipment. But sometimes they were rolled up and inserted into the open ends of scaffold poles.

One day a man put a permit into the open end of a pipe. He probably thought that it was a scaffold pole or defunct pipe. Unfortunately it was the air bleed into a vacuum system. The air rate was controlled by a motor valve. The permit got sucked into the valve and blocked it. The vacuum could not be broken, product was sucked into the vacuum system, and the plant had to be shut down for cleaning for two days.

(c) Section 2.3 described some of the results of moving people.

2.9 GRADUAL CHANGES

These are the most difficult to control. Often, we do not realize that a change is taking place until it is too late. For example, over the years, steam consumption at a plant had gradually fallen. Flows through the mains became too low to prevent condensate accumulating. On one of the mains, an inaccessible steam trap had been isolated, and the other main had settled slightly. Neither of these mattered when the steam flow was large, but it gradually fell. Condensate accumulated, and finally water hammer fractured the mains.

Oil fields that produce sweet (that is, hydrogen-sulfide-free) oil and gas can gradually become sour. If this is not detected in time, there can be risks to life and unexpected corrosion.

In ammonia plants, the furnace tubes end in pigtails—flexible pipes that allow expansion to take place. On one plant, over the years, many small changes were made to pigtails' design. The net effect was to shorten the bending length and thus increase the stress. Ultimately 54 tubes failed, producing a spectacular fire [9].

In the UK, cars are usually about 53 in. (1.35 m) high. During the 1990s a number of taller models were introduced with heights of 62–70 in. (1.6–1.8 m). They gave better visibility, but the center of gravity rose, and the cars became less stable when cornering. An expensive model had to be withdrawn for modification [38].

Most incidents have occurred before. In 1906, in the UK, there was a sharp curve in the railway line outside Salisbury rail station. The speed limit was 30 mph, but drivers of trains that did not stop at the station often went faster. A new design of engine was introduced, similar to those already in use but with a larger boiler and thus a higher center of gravity. When it was driven around the curve at excessive speed, the train came off the rails, killing 28 people. Afterward all trains were required to stop at the station [39].

2.10 MODIFICATION CHAINS

We make a small change to a plant or new design. A few weeks or months later we realize that the change had or will have a consequence we did not foresee and a further change is required; later still, further changes are required, and in the end we may wish we had never made the original change, but it may be too late to go back.

For example, small leaks through relief valves may cause pollution, so rupture discs were fitted below the relief valves (Figure 2-11 a). (On other occasions they have been fitted to prevent corrosion of the relief valves.) It was soon realized that if there is a pinhole in a rupture disc, the pressure in the space between the disc and the relief valve will rise until it is the same as the pressure below the disc. The disc will then not rupture until the pressure below it rises to about twice the design rupture pressure. Therefore, to prevent the interspace pressure rising, small vents to atmosphere were fitted between the discs and the relief valves (Figure 2-11 b).

This is okay if the disc is there to prevent corrosion, but if the disc is intended to prevent pollution, it defeats the object of the disc. Pressure gauges were therefore fitted to the vents and the operators asked to read them every few hours (Figure 2-11 c).

Many of the relief valves were on the tops of distillation columns and other high points, so the operators were reluctant to read the pressure gauges. They were therefore brought down to ground level and connected to the vents by long lengths of narrow pipe (Figure 2-11 d).

These long lengths of pipe got broken or kinked or liquid collected in them. Sometimes operators disconnected them so the pressure always read zero. The gauges and long lengths of pipe were therefore replaced by excess flow valves, which vent small leaks from pinholes but close if the rupture disc ruptures (Figure 2-11 e).

Unfortunately, the excess flow valves were fitted with female threads, and many operators are trained to screw plugs into any open female threads they see. So some of the excess flow valves became plugged.

Pressure transmitters, alarming in the control room, were therefore fitted in place of the excess flow valves (Figure 2-11 f). This was an expensive solution. Perhaps it would be better to remove the rupture discs and prevent leaks to the atmosphere by taking more care over the machining and lapping of the relief valves.

A tank truck containing liquefied petroleum gas was fitted with a rupture disc below its relief valve, and a pressure gauge was fitted to the interspace. When it arrived at its destination, in Thailand, the customer telephoned the supplier, in Holland, to say the tank was empty, as the pressure gauge read zero [10].

For other examples of modification chains, see References 11 and 12.

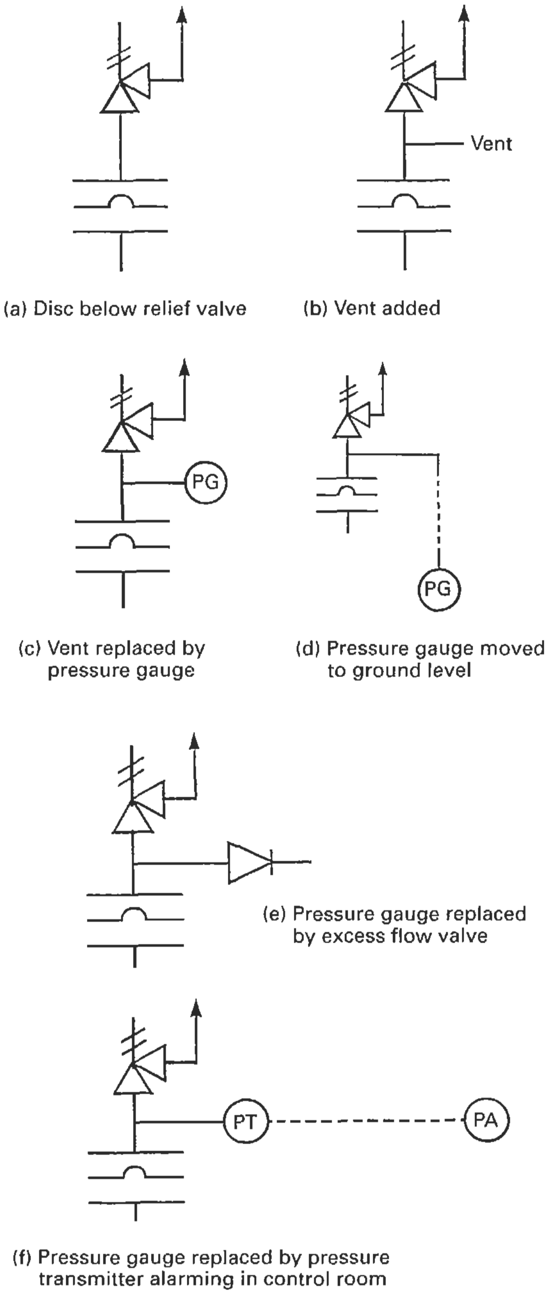


Figure 2-11. A modification chain—rupture discs below relief valves.

2.11 MODIFICATIONS MADE TO IMPROVE THE ENVIRONMENT

Modifications made to improve the environment have sometimes produced unforeseen hazards [16]. We should, of course, try to improve the environment, but before making any changes we should try to foresee their results, as described in Section 2.12.

2.11.1 Explosions in Compressor Houses

A number of compressor houses and other buildings have been destroyed or seriously damaged, and the occupants killed, when leaks of flammable gas or vapor have exploded. Indoors, a building can be destroyed by the explosion of a few tens of kilograms of flammable gas, but outdoors, several tons or tens of tons are needed. During the 1960s and 1970s, most new compressor houses and many other buildings in which flammable materials were handled were built without walls so that natural ventilation could disperse any leaks that occurred; the walls of many existing buildings were pullled down.

In recent years, many closed buildings have again been built in order to meet new noise regulations. The buildings are usually provided with forced ventilation, but this is much less effective than natural ventilation and is usually designed for the comfort of the operators rather than the dispersion of leaks.

The noise radiation from compressors can be reduced in other ways, for example, by surrounding the compressor with acoustic insulation. Any gap between the compressor and the insulation should be purged with air.

The leaks that lead to explosions in compressor houses are often not from a compressor but from other equipment, such as pipe joints. One such leak occurred because a spiral-wound gasket had been replaced by a compressed asbestos fiber one, probably as temporary measure, seven years earlier. Once installed, it was replaced by a similar one during subsequent maintenance [30].

Another explosion, which killed one man and destroyed three natural gas compressors and the building housing them, started when five of the eight nuts that held a bypass cap on a suction valve failed, as the result of fatigue. They had been overtightened. The emergency shutdown system failed to operate when gas was detected and again when an attempt was

made to operate it manually. It was checked only once per year. The source of ignition was believed to be the electrical equipment on the gas engine that drove the compressor [31].

In recent years there has been a rapid growth in the number of combined heat and power (CHP) and combined cycle gas turbine (CCGT) plants, driven mainly by gas turbines using natural gas, sometimes with liquid fuel available as stand-by. Governments have encouraged the construction of these plants, as their efficiency is high and they produce less carbon dioxide than conventional coal and oil-burning power stations. However, they present some hazards, as gas turbines are noisy and are therefore usually enclosed.

In addition, they are usually constructed without isolation valves on the fuel supply lines. As a result the final connection in the pipework cannot be leak-tested. In practice, it is tested as far as possible at the manufacturer's works but often not leak-tested on-site. Reference 32 reviews the fuel leaks that have occurred, including a major explosion at a CCGT plant in England in 1996 due to the explosion of a leak of naphtha from a pipe joint. One man was seriously injured, and a 600-m^3 chamber was lifted off its foundations. The reference also reviews the precautions that should be taken. They include selecting a site where noise reduction is not required or can be achieved without enclosure. If enclosure is essential, then a high ventilation rate is needed; it is often designed to keep the turbine cool and is far too low to disperse gas leaks. Care must be taken to avoid stagnant pockets.

A reaction occasionally ran away and released vapor through a vent into the surrounding building. The vapor condensed to form a flammable fog. It had never been known to ignite, but nevertheless the company issued a strong but nonbinding recommendation that the walls of the building should be removed. One plant decided not to follow the recommendation. As a result most of the walls were removed by an explosion. The source of ignition was never found [33].

2.11.2 Aerosols and Other Uses of CFCs

During the 1980s, it became recognized that chlorofluorocarbons (CFCs), widely used as aerosol propellants, are damaging the ozone layer, and aerosol manufacturers were asked to use other propellants. Some

manufacturers already used butane, a cheaper material, and other manufacturers started to use it. The result was a series of fires and explosions.

The change was made quickly with little consideration of the hazards of handling butane. The reports on some of the fires that occurred say the hazards were not understood and that elementary safety precautions were lacking. One United Kingdom company was prosecuted for failing to train employees in the hazards of butane, in fire evacuation procedures, and in emergency shutdown procedures. These actions were, of course, not necessary or less necessary when CFCs were used. Following this fire, factory inspectors visited other aerosol factories and found much that could be improved. The manufacturers of the filling machines agreed to modify them so that they would be suitable for handling butane. This, apparently, had not been considered before.

CFCs have been widely used as cleaning solvents, as they are nonflammable and their toxicity is low. Now, flammable solvents are coming back into favor. A news item from a manufacturer described "a new ozone-friendly cleaning process for the electronics industry," which "uses a unique hydrocarbon-alcohol formulation." It did not remind readers that the mixture is flammable and that they should check that their equipment and procedures are suitable.

Bromochlorofluorocarbons (BCFs or halons) have been widely used for fire fighting. They were considered wonder chemicals when first used, but their manufacture has now ceased, though existing stocks may still be used. Alternative, though less effective, materials, such as fluorinated hydrocarbons, are available. Let us hope there will not be a return to the use of carbon dioxide for the automatic protection of rooms containing electrical equipment. If the carbon dioxide is accidentally discharged while someone is in the room, they will be asphyxiated, but accidental discharge of halon will not cause serious harm. Of course, procedures require the carbon dioxide supply to be isolated before anyone enters the room, but these procedures have been known to break down.

A liquid chlorine tank was kept cool by a refrigeration system that used CFCs. In 1976 the local management decided to use ammonia instead. Management was unaware that ammonia and chlorine react to form explosive nitrogen trichloride. Some of the ammonia leaked into the chlorine, and the nitrogen trichloride that was formed exploded in a pipeline

connected to the tank; six men were killed, though the report does not say whether they were killed by the explosion or by the chlorine.

2.11.3 Vent Systems

During the 1970s and 1980s there was increasing pressure to collect the discharges from tank vents, gasoline filling, etc., for destruction or absorption, instead of discharging them into the atmosphere, particularly in areas subject to photochemical smog. A 1976 report said that when gasoline recovery systems were installed in the San Diego area, more than 20 fires occurred in four months. In time, the problems were overcome, but it seems that the recovery systems were introduced too quickly and without sufficient testing.

As vent collection systems normally contain vapor/air mixtures, they are inherently unsafe. They normally operate outside the flammable range, and precautions are taken to prevent them from entering it, but it is difficult to think of everything that might go wrong. For example, an explosion occurred in a system that collected flammable vapor and air from the vents on a number of tanks and fed the mixture into a furnace. The system was designed to run at 10% of the lower explosion limit, but when the system was isolated in error, the vapor concentration rose. When the flow was restored, a plug of rich gas was fed into the furnace, where it mixed with air and exploded [17]. Reference 34 describes ten other incidents.

At other times the burning of waste products in furnaces to save fuel and reduce pollution has caused corrosion and tube failure.

A fire in a bulk storage facility at Coode Island, Melbourne, Australia, in August 1991 caused extensive damage and many complaints about the pollution caused by the smoke plume, but no injuries. The tank vents were connected together and piped to a carbon bed vapor recovery system. There were no flame arrestors in the pipework. Whatever the cause of the initial fire or explosion, the vent collection system provided a means of spreading the fire from one tank to another.

In the past it was difficult to prevent the spread of explosions through vent systems, as flame arrestors were effective only when located at the ends of pipes. Effective inline detonation arrestors are now availabe. Like all flame arrestors they will, of course, need regular cleaning, something that is often neglected. In other cases, when tanks have been over-

filled, liquid has contaminated other tanks through common vent systems, and this has led to runaway reactions.

Carbon beds are often used for absorbing vapors in vent systems but absorption produces heating, and the beds may catch fire, particularly if they are used to absorb ketones, aldehydes organic, acids, and organic sulfur compounds. References 35–37 describe some fires and ways of preventing them.

In 1984, an explosion in a water pumping station at Abbeystead, UK, killed 16 people, most of them local residents who were visiting the plant. Water was pumped from one river to another through a tunnel. When pumping was stopped, some water was allowed to drain out of the tunnel and leave a void. Methane from the rocks below accumulated in the void and, when pumping was restarted, was pushed through vent valves into a valvehouse, where it exploded [18].

It is surprising that the vent was routed into an underground pumphouse. It seems that this was done because the local authority objected to any vents that might spoil the view.

A small factory in a residential area in the UK recovered solvent by distillation. The cooling water supply to the condenser, after giving trouble for several weeks, finally failed, and hot vapors were discharged from a vent inside a building. They exploded, killing one man, injuring another, and seriously damaging the factory. Some of the surrounding houses were slightly damaged, and five drums landed outside the factory, one on a house.

There were no operating or emergency instructions and no indication of cooling water flow, and drums were stored too near buildings. But, by far, the most serious error was allowing the vent pipe to discharge inside the building. If it had discharged outside, the vapor would have dispersed harmlessly, or at worst, there would have been a small fire on the end of the vent pipe. Vent pipes are designed to vent, so this was not an unforeseen leak. The vent pipe may have been placed indoors to try to minimize smells that had caused some complaints [19].

Increasingly, safety, health, and the environment are becoming parts of the same SHE department in industry. This should help to avoid incidents such as those described in Section 2.11. Unfortunately, there are few signs of a similar integration in government departments.

2.12 CONTROL OF MODIFICATIONS

How can we prevent modifications from producing unforeseen and undesirable side effects? References 1 and 2 propose a three-pronged approach:

(1) Before any modification, however inexpensive, temporary or permanent, is made to a plant or process or to a safety procedure, it should be authorized in writing by a process engineer (plant manager in the UK) and a maintenance engineer, that is, by professionally qualified staff, usually the first level of professionally qualified staff. Before authorizing the modification, they should make sure there will be no unforeseen consequences and that it is in accordance with safety and engineering standards. When the modification is complete, they should inspect it to make sure their intentions have been followed and that it "looks right." What does not look right is usually not right and should at least be checked.

(2) The managers and engineers who authorize modifications cannot be expected to stare at a drawing and hope that the consequences will show up. They must be provided with an aid, such as a list of questions to be answered. Such an aid is shown in References 1 and 2. Large or complex modifications should be subjected to a hazard and operability study (see Chapter 18).

(3) It is not sufficient to issue instructions about (1) and the aid described in (2). We must convince all concerned, particularly foremen, that they should not carry out unauthorized modifications. This can be done by discussing typical incidents, such as those described here; those illustrated in the Institution of Chemical Engineers (UK) Safety Training Package No. 025, *Modifications—The Management of Change;* or better still, incidents that have occurred in your own company.

To paraphrase an old fable, Midas asked the gods that everything he touched might be turned to gold. His request was granted. His food turned to gold the moment he touched it, and he had to ask the gods to take their favor back.

REFERENCES

1. T. A. Kletz, *Chemical Engineering Progress,* Vol. 72, No. 11, Nov. 1976, p. 48.
2. F. P. Lees, *Loss Prevention in the Process Industries,* 2nd edition, Butterworth-Heinemann, Oxford, UK, 1996, Chapter 21.
3. *The Flixborough Cyclohexane Disaster,* Her Majesty's Stationery Office, London, 1975.
4. *Guide Notes on the Safe Use of Stainless Steel.* Institution of Chemical Engineers, Rugby, UK, 1978.
5. A note issued by the U.S. National Transportation Safety Board on Nov. 12, 1976.
6. *Chemical Safety Summary,* Vol. 56, No. 221, Chemical Industries Association, London, 1985, p. 6.
7. L. Silver, *Loss Prevention,* Vol. 1, 1967, p. 58.
8. A. H. Searson, *Loss Prevention,* Vol. 6, 1972, p. 58.
9. C. S. McCoy, M. D. Dillenback, and D. J. Truax, *Plant/Operations Progress,* Vol. 5, No. 3, July 1986, p. 165.
10. *Hazardous Cargo Bulletin,* Jan. 1985, p. 31.
11. T. A. Kletz, *Plant/Operations Progress,* Vol. 5, No. 3, July 1986, p. 136.
12. R. E. Sanders, *Management of Change in Chemical Plants—Learning from Case Histories,* Butterworth-Heinemann, Oxford, UK, 1993.
13. *Loss Prevention Bulletin,* No. 098, Apr. 1991, p. 13.
14. S. J. Skinner, *Plant/Operations Progress,* Vol. 8, No. 4, Oct. 1989, p. 211.
15. D. Mosey, *Reactor Accidents,* Butterworth Scientific, London, 1990, p. 45.
16. T. A. Kletz, *Process Safety Progress,* Vol. 12, No. 3, July 1993, p. 147.
17. S. E. Anderson, A. M. Dowell, and J. B. Mynagh, *Plant/Operations Progress,* Vol. 11, No. 2, Apr. 1992, p. 85.
18. Health and Safety Executive, *The Abbeystead Explosion,* Her Majesty's Stationery Office, London, 1985.

19. Health and Safety Executive, *The Explosion and Fire at Chemstar Ltd., 6 September 1981,* Her Majesty's Stationery Office, London, 1982.
20. *Operating Experience Weekly Summary,* No. 96-47, Office of Nuclear and Safety Facility, U.S. Dept. of Energy, Washington, D.C., 1996, p. 3.
21. *Operating Experience Weekly Summary,* No. 96-52, Office of Nuclear and Safety Facility, U.S. Dept. of Energy, Washington, D.C., 1996, p. 8.
22. S. J. Brown, *Plant/Operations Progress,* Vol. 5, No. 11, Jan. 1987, p. 20.
23. R. E. Sanders, *Plant/Operations Progress,* Vol. 15, No. 3, Fall 1996, p. 150.
24. *Loss Prevention Bulletin,* No. 119, Oct. 1994, p. 17.
25. T. A. Kletz, *Learning from Accidents,* 2nd edition, Butterworth-Heinemann, 1994, Chapter 8.
26. F. P. Lees, *Loss Prevention in the Process Industries,* 2nd edition, Butterworth-Heinemann, 1996, Appendix 2.
27. *Operating Experience Weekly Summary,* No. 97-01, Office of Nuclear and Facility Safety, U.S. Dept. of Energy, Washington, D.C., 1997, p. 2.
28. W. Zacky, Remarks made at 2nd biennial Canadian Conference on Process Safety and Loss Management, Toronto, Canada, June 1995.
29. C. Whetton and P-J. Bots, *Loss Prevention Bulletin,* No. 128, Apr. 1996, p. 7.
30. J. A. McDiarmid and G.J.T. North, *Plant/Operations Progress,* Vol. 8, No. 2, 1989, p. 96.
31. *Loss Prevention Bulletin,* No. 127, p. 6.
32. R. C. Santon, "Explosion Hazards at CHP and CCGT Plants," *Hazards XIII: Process Safety—The Future,* Symposium Series No. 141, Institution of Chemical Engineers, Rugby, UK, 1997.
33. W. B. Howard, "Case Histories of Two Incidents Following Process Safety Reviews," *Proceedings of the Thirty-first Annual Loss Prevention Symposium,* AIChE, New York, 1997.

34. F. E. Self and J. D. Hill, "Safety Considerations When Treating VOC Streams with Thermal Oxidizers," *Proceedings of the Thirty-first Annual Loss Prevention Symposium,* AIChE, New York, 1997.

35. M. J. Chapman and D. L. Field, *Loss Prevention,* Vol. 12, 1979, p. 136, including discussion.

36. R. E. Sherman, et al., *Process Safety Progress,* Vol. 15, No. 3, Fall 1996, p. 148.

37. G. R. Astbury, *Loss Prevention Bulletin,* No. 134, Apr. 1997, p. 7.

38. *Daily Telegraph* (London), Motoring Supplement, Nov. 22, 1997, p. C1.

39. S. Hall, *British Railway Disasters,* Ian Allan, Shepperton, UK, p. 178.

Chapter 3

Accidents Caused by Human Error

Teach us, Lord, to accept the limitations of man.

—*Forms of Prayer for Jewish Worship*

3.1 INTRODUCTION

This chapter describes accidents caused by those slips and lapses of attention that even well-trained and well-motivated persons make from time to time. For example, they forget to close a valve or close the wrong valve. They know what they should do, want to do it, and are physically and mentally capable of doing it. But they forget to do it. Exhortation, punishment, or further training will have no effect. We must either accept an occasional error or change the work situation so as to remove the opportunities for error or to make errors less likely.

These errors occur, not in spite of the fact that someone is well-trained but *because* he or she is well-trained. Routine operations are relegated to the lower levels of the brain and are not continuously monitored by the conscious mind. We would never get through the day if everything we did required our full attention. When the normal pattern or program of actions is interrupted for any reason, errors are likely to occur. These slips are very similar to those we make in everyday life. Reason and Mycielska [1] have described the psychology of such slips.

We then describe some accidents that occurred because employees were not adequately trained (mistakes). Sometimes they lacked basic knowledge; sometimes they lacked sophisticated skills.

Errors also occur because people deliberately decide not to carry out instructions that they consider unnecessary or incorrect. These are called violations. For example, they may not wear all the protective clothing or take the other precautions specified on a permit-to-work, as discussed in Section 1.4.2. We should ask the following questions both before and after accidents of this type:

- Are the rules known and understood? Is it possible to follow them?
- Are the rules, such as wearing protective clothing, really necessary? See Section 1.4.2 (a).
- Can the job be simplified? If the correct method is difficult, and an incorrect method is easy, people are likely to use the incorrect method.
- Do people understand the reasons for the rules? We do not live in a society in which people will follow the rules just because they are told to do so.
- Have breaches of the rules been ignored in the past?
- There is a narrow line between initiative and rule breaking. What would have happened if no accident had occurred?

3.2 ACCIDENTS CAUSED BY SIMPLE SLIPS. TO PREVENT THEM WE SHOULD CHANGE THE PLANT DESIGN OR METHOD OF WORKING.

3.2.1 "There is Nothing Wrong With The Design. The Equipment Wasn't Assembled Correctly."

How often has this been said by the designer after a piece of equipment has failed? The designer is usually correct, but whenever possible we should use designs that are impossible (or difficult) to assemble incorrectly or that are unlikely to fail if assembled incorrectly. For example:

(a) In some compressors it is possible to interchange suction and delivery valves. Damage and leaks have developed as a result. Valves should be designed so they cannot be interchanged.

(b) With many types of screwed couplings and compression couplings, it is easy to use the wrong ring. Accidents have occurred as a result. Flanged or welded pipes should therefore be used except on small-bore lines carrying nonhazardous materials.

(c) Loose-backing flanges require more care during joint making than fixed flanges. Fixed flanges are therefore preferred.

(d) Bellows (expansion joints) should be installed with great care, because unless specially designed, they cannot withstand any sideways thrust. With hazardous materials, it is therefore good practice to avoid the need for bellows by designing expansion bends into the pipework.

(e) A runaway reaction occurred in a polymerization reactor. A rupture disc failed to burst. It had been fitted on the wrong side of the vacuum support, thus raising its bursting pressure from a gauge pressure of 150 psi (10 bar) to about 400 psi (27 bar) (Figures 3-1a and 3-1b).

The polymer escaped through some of the flanged joints, burying the reactor in a brown polymer that looked like molasses candy (treacle toffee). The reactor was fitted with class 150 flanges. If these are overpressured, the bolts will stretch, and the flanges will leak, thus preventing the vessel from bursting (provided the pressure does not rise too rapidly). But this may not occur with flanges of a higher pressure rating.

The best way to prevent accidents such as this is to use rupture discs, which are harder to assemble incorrectly and which can be checked for correct installation after assembly. It is possible to get discs permanently attached to their vacuum supports by the manufacturer and fitted with a projecting tag, which carries the words *vent side* on one side. The tag also gives the pressure rating.

A small rupture disc failed to operate; it was then found that the manufacturer had inadvertently supplied two discs that nested one on top of the other and appeared to be one. Most discs are individually boxed, but some are supplied stacked and should be carefully checked. Some small discs are supplied with gaskets already glued to them, and these are particularly likely to stick together.

(See Section 5.3 g and Section 9.1.3.)

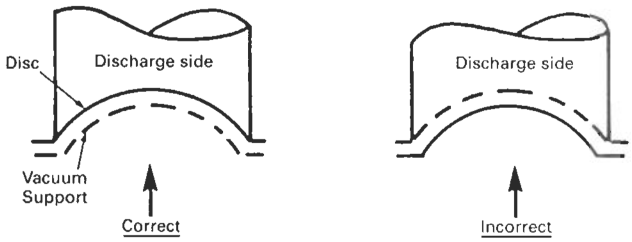


Figure 3-1a. Arrangements of rupture disc and vacuum support.

Figure 3-1b. Because a rupture disc was fitted to the wrong side of a vacuum support, the flanges leaked, covering the reactor with "candy."

3.2.2 Wrong Valve Opened

The pump feeding an oil stream to the tubes of a furnace failed. The operator closed the oil valve and intended to open a steam valve to purge the furnace tubes. He opened the wrong valve, there was no flow to the furnace, and the tubes were overheated and collapsed.

This incident is typical of those that would at one time have been blamed on human failing—the operator was at fault, and there was nothing anyone else could have done. In fact investigation showed that:

1. The access to the steam valve was poor, and it was difficult to see which was the right valve.
2. There was no indication in the control room to show that there was no flow through the furnace coils.
3. There was no low-flow alarm or trip on the furnace.

3.2.3 Would You Climb Over a Pipe or Walk 90 m?

To repair a flowmeter, a man had to walk six times from the orifice plate to the transmitter and back. To get from one to the other, he had to walk 45 m, cross a 30-in.-diameter pipe by a footbridge, and walk 45 m back—a total of 540 m for the whole job. Instead, he climbed over the pipe; while doing so he hurt his back.

Is it reasonable to expect a man to repeatedly walk 90 m to avoid climbing over a pipe?

3.2.4 An Error While Testing A Trip

Two furnaces were each fitted with a temperature recorder controller and high-temperature trip. The two recorders were side by side on the instrument panel in the control room, with the recorder for A furnace on the left (Figure 3-2).

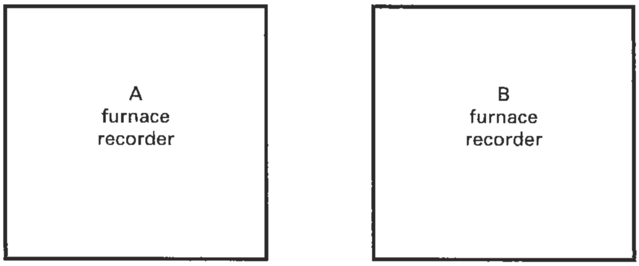


Figure 3-2. Layout of recorders on panel.

An instrument mechanic was asked to test the trip on A furnace. He put the controller on manual and then went behind the panel. His next step was to take the cover off the back of the controller, disconnect one of the leads, apply a gradually increasing potential from a potentiometer, and note the reading at which the trip would operate if it was on auto control.

The mechanic, who had done the job many times before, took the cover off the back of B recorder, the one on the left behind the panel (Figure 3-3), and disconnected one of the leads. The effect was the same as if the recorder had registered a high temperature. The controller closed the fuel gas valve, shutting down the furnace and the rest of the plant.

We all know that the recorder on the left, viewed from the front of the panel, will be on the right when viewed from behind the panel, but the mechanic had his mind set on "the one on the left."

The backs of the two recorders should have been labeled A and B in large letters. Better still, the connections for the potentiometer should have been at the front of the panel.

3.2.5 Poor Layout of Instructions

A batch went wrong. Investigation showed that the operator had charged 104 kg of one constituent instead of 104 g (0.104 kg).

The instructions to the operator were set out as shown in Table 3-1 (the names of the ingredients being changed):

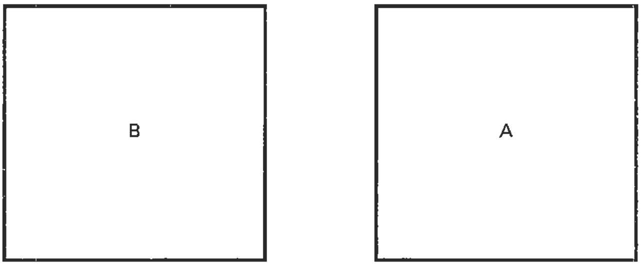


Figure 3-3. Layout of recorders behind panel.

Table 3-1
Operator Instructions

Blending Ingredients	Quantity (tons)
Marmalade	3.75
Oxtail soup	0.250
Pepper	0.104 kg
Baked beans	0.020
Raspberry jam	0.006
TOTAL	4.026

With instructions like these it is very easy for the operator to get confused.

3.2.6 An Inaccurate Reading Not Noticed on an Instrument at Thigh Level

A reactor was being started up. It was filled with reaction mixture from another reactor, which was already on line, and the panel operator started to add fresh feed, gradually increasing the flow while he watched the temperature on a recorder conveniently situated at eye level. He intended to start a flow of cooling water to the reaction cooler as soon as the temperature started to rise—the usual method.

Unfortunately, there was a fault in the temperature recorder, and although the temperature actually rose, this was not indicated. Result: a runaway reaction.

The rise in temperature was, however, indicated on a six-point temperature recorder at a lower level on the panel, but the operator did not notice this (Figure 3-4).

An interesting feature of this incident was that no one blamed the operator. The manager said he would probably have made the same mistake because the check instrument was at a low level (about 1 m above the floor) and because a change in one temperature on a six-point recorder in that position is not obvious unless you are actually looking for it. It is not the sort of thing you notice out of the corner of your eye.

3.2.7 Closing Valves in Error

(a) Figure 3-5 shows part of a plant in which five reactors were in parallel. There were two gas-feed lines with cross connections

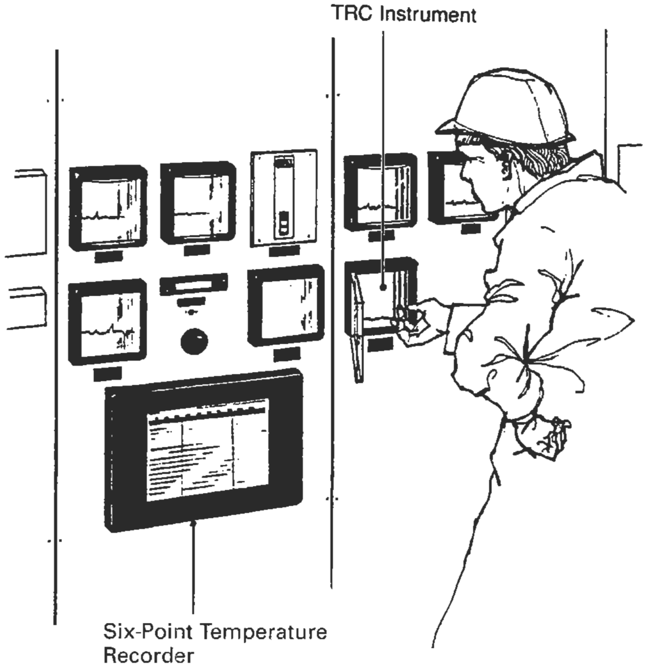


Figure 3-4. Instruments below eye level may not be noticed.

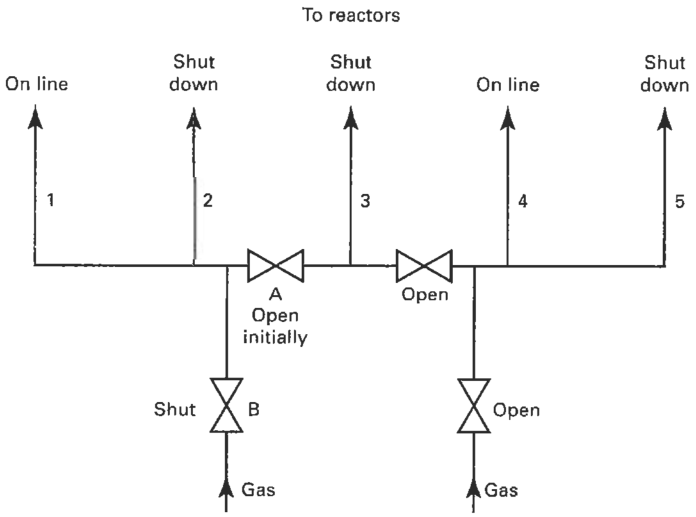


Figure 3-5. Accidental closing of a valve can cause an explosion.

between them. Oxygen was also fed to the reactors, but the oxygen lines are not shown. At the time of the incident only two reactors, Nos. 1 and 4, were on line.

The operator thought valve B was open, so he shut valve A. This stopped the flow of gas to No. 1 reactor. The oxygen flow was controlled by a ratio controller, but it had a zero error, and a small flow of oxygen continued.

When the operator realized his mistake and restored the gas flow, the reactor contained excess oxygen, and an explosion occurred, not actually in the reactor but in the downstream waste heat boiler. Four men were killed.

Here we have a situation where simple error by an operator produced serious consequences. The explosion was not, however, the operator's fault but was the result of bad design and lack of protective equipment.

We would never knowingly tolerate a situation in which accidental operation of a valve resulted in the overpressuring of a vessel. We would install a relief valve. In the same way, accidental operation of a valve should not be allowed to result in explosion or runaway reaction.

(b) The switch in the power supply to a safety interlock system was normally locked in the closed position, even during shutdowns, to prevent accidental isolation. One day an operator was asked to lock it open. He was so used to locking it shut that he locked it in the wrong position. Breaking a habit is difficult. Another operator who was asked to check did not spot the error. As seen in Sections 1.2.3 (e) and 14.5 (c), checking is often ineffective, because the checker expects to find everything in order. According to the report [7] the operators were disciplined, but this will not prevent another incident, as the errors were not deliberate. A better method of working might involve using a key that can be removed only when the switch is in one position.

This incident occurred in a nuclear power station but could just as easily occur in the process industries.

3.2.8 An Explosion in a Batch Reactor

Figure 3-6 shows a batch reaction system. A batch of glycerol was placed in the reactor and circulated through a heat exchanger, which

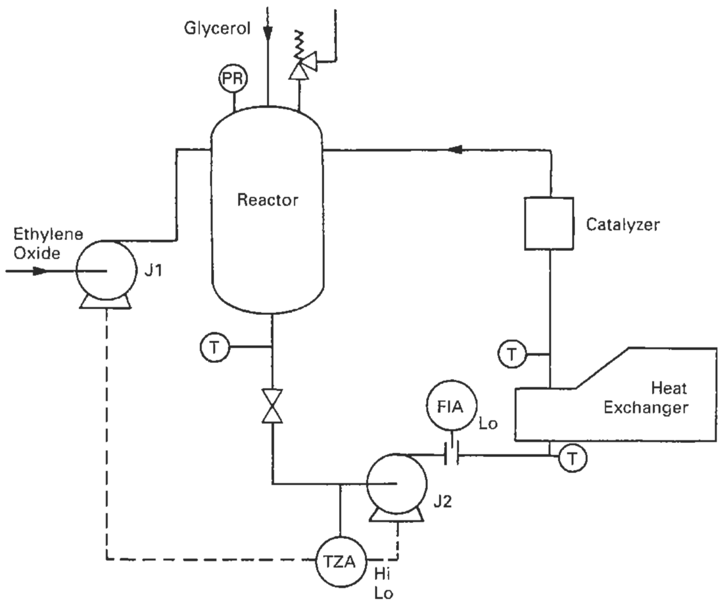


Figure 3-6. Arrangements of reactor circulating system.

could act as both a heater and a cooler. Initially it was used as a heater, and when the temperature reached 115°C, addition of ethylene oxide was started. The reaction was exothermic, and the exchanger was now used as a cooler.

The ethylene oxide pump could not be started unless:

1. The circulation pump was running.
2. The temperature was above 115°C, as otherwise the ethylene oxide would not react.
3. The temperature was below 125°C, as otherwise the reaction was too fast.

Despite these precautions, an explosion occurred. One day, when ethylene oxide addition was started, the pressure in the reactor rose. This showed that the ethylene oxide was not reacting. The operator decided that perhaps the temperature point was reading low or perhaps a bit more heat was required to start the reaction, so he adjusted the trip setting and allowed the indicated temperature to rise to 200°C. Still the pressure did not fall.

He then suspected that his theory might be wrong. Could he have forgotten to open the valve at the base of the reactor? He found it shut and opened it. Three tons of unreacted ethylene oxide; together with the glycerol, passed through the heater and catalyzer, and a violent, uncontrolled reaction occurred. The reactor burst, and the escaping gases exploded. Two men were injured. One, 160 m away, was hit by flying debris, and the other was blown off the top of a tank truck.

Although the indicated temperature had risen, the temperature of the reactor's contents had not. Pump J2, running with a closed suction valve, got hot, and the heat affected the temperature point, which was close to the pump.

Why did it happen?

1. The immediate cause of the explosion was an operator forgetting to open a valve. It was not due to lack of knowledge, training, or instructions but was another of those slips that even well-trained, well-motivated, capable people make from time to time.
2. If the operator had not opened the valve when he found it shut, the explosion could have been avoided. However, it is hard to blame him. His action was instinctive. What would you do if you found something undone that you should have done some time ago?
3. The explosion was due to a failure to heed warning signs. The high pressure in the reactor was an early warning, but the operator had another theory to explain it. He stuck to this theory until the evidence against it was overwhelming. This is known as a mind-set or tunnel vision.

   The other temperature points would have helped the operator diagnose the trouble. But he did not look at them. He probably thought there was no point in doing so. All the temperature points were bound to read the same. The need for checking one reading by another should have been covered in the operator's training.
4. The explosion was due to a failure to directly measure the property that we wish to know. The temperature point was not measuring the temperature in the reactor but the temperature near the pump. This got hot because the pump was running with a closed suction valve. Similarly, the trip initiator on J2 showed that its motor was energized. It did not prove that there was a flow.

5. The explosion occurred because key instruments were not kept in working order. The flow indicator and low flow alarm (FIA) were out of order. They often were, and the operators had found that the plant could be operated without them. If there is no flow, they thought, J2 will have stopped, and this will stop J1.
6. The operator should not have raised the interlock setting, though doing so did not in itself cause the explosion. (However, he did try to use his intelligence and think why the reaction was not occurring. Unfortunately, he was wrong.)

What should we do?

It is no use telling the operator to be more careful. We have to recognize that the possibility of an error—forgetting to open the valve—is inherent in the work situation. If we want to prevent an error, we must change the work situation. That is, change the design and/or the method of operation—the hardware and/or the software.

The original report blamed the operator for the explosion. But his failure to open the valve might have been foreseen.

1. The temperature should be measured in the reactor or as close to it as possible. We should always try to measure the property we wish to know directly, rather than measuring another property from which the property we wish to know can be inferred.

   The designers assumed that the temperature near the pump would be the same as that in the reactor. It will not be if there is no circulation.

   The designers assumed that if the pump is energized, then liquid is circulating, but this is not always the case.
2. Operators should not be allowed to change trip settings at will. Different temperatures are needed for different batches. But even so, the adjustment should be made only by someone who is given written permission to do so.
3. More effort might have been made to keep the flow indicator alarm in working order.
4. A high-pressure trip should be installed on the reactor.

5. Operators should be trained to "look before they leap" when they find valves wrongly set. See also Section 3.3.5 (a). Other accidents that occurred because operators failed to carry out simple tasks are described in Sections 13.5 and 17.1.

3.3 ACCIDENTS THAT COULD BE PREVENTED BY BETTER TRAINING

As we shall see, very often it is not a lack of sophisticated training that results in accidents but ignorance of the basic requirements of the job or the basic properties of the materials and equipment handled.

3.3.1 Readings Ignored

Many accidents have occurred because operators apparently thought their job was just to write down readings and not to respond to them.

(a) The temperature controller on the base of a distillation column went out of order at 5 a.m. and drew a straight line. This was not noticed. During the next seven hours the following readings were abnormal:

1. Six tray temperatures (one rose from 145°C to 255°C)
2. Level in base of still (low)
3. Level in reflux drum (high)
4. Take-off rate from reflux drum (high)

Most of these parameters were recorded on the panel. All were written down by the operator on the record sheet.

Finally, at 12 noon, the reflux drum overflowed, and there was a spillage of flammable oil. From 7 a.m. onward, a trainee served as operator, but a lead operator was present, and the foreman visited the control room from time to time.

(b) Section 2.5 (a) describes how a low-pressure liquefied ethylene storage tank split when the vent pipe became plugged with ice. For 11 hours before the split occurred, the gauge pressure in the tank was reading 2 psi (0.13 bar). This pressure was above the set-point of the relief valve (a gauge pressure of 1.5 psi, or 0.1 bar) and was the full-scale reading on the pressure gauge. The operators entered this reading on the record sheet but took no other action and did

not even draw it to the attention of the foremen or managers when they visited the control room [2]. Section 8.1.6 describes a similar incident.

(c) The governor assembly and guard on a steam engine disintegrated with a loud bang, scattering bits over the floor. Fortunately no one was injured. It was then found that the lubricating oil gauge pressure had been only 8 psi (0.5 bar) instead of 25 psi (1.7 bar) for at least "several months." In this case the pressure was not written down on the record sheet.

(d) The level measuring instrument and alarm on a feed tank were out of order, so the tank was hand-dipped every shift. When the plant was shut down, the operators stopped dipping the tank. The plant that supplied the feed was not shut down. It continued to supply feed into the feed tank until it overflowed. In this case readings were not ignored but simply not taken. There were some errors in the stock sheets, and the tank contained more than expected. However, if the operators had continued to dip the tank every shift, the error would have been detected before the tank overflowed.

How can we prevent similar incidents from happening again?

1. Emphasize in operator training that operators should take action on unusual readings, not just write them down. Make sure they know the action to take.
2. Mark control limits in red on record sheets. If readings are outside these limits, some action is required.
3. Continue to take certain readings, such as tank levels, even when the plant is shut down. Tank levels are particularly liable to rise or fall when they should be steady.

3.3.2 Warnings Ignored

When a warning is received, many operators are too ready to assume the alarm is out of order. They thus ignore it or send for the instrument mechanic. By the time the mechanic confirms that the alarm is correct, it is too late. For example:

(a) During the morning shift, an operator noticed that a tank level was falling faster than usual. He reported that the level gauge was out

of order and asked an instrument mechanic to check it. It was afternoon before the mechanic could do so. He reported that it was correct. The operator then looked around and found a leaking drain valve. Ten tons of material had been lost.

(b) After making some modifications to a pump, the pump was used to transfer some liquid. When the transfer was complete, the operator pressed the Stop button on the control panel and saw that the Pump Running light went out. He also closed a remotely operated valve in the pump delivery line.

Several hours later, the high-temperature alarm on the pump sounded. Because the operator had stopped the pump and seen the Pump Running light go out, he assumed the alarm was faulty and ignored it. Soon afterward an explosion occurred in the pump.

When the pump was modified, an error was introduced into the circuit. As a result, pressing the Stop button did not stop the pump but merely switched off the Pump Running light. The pump continued running against a closed delivery valve, overheated, and the material in it decomposed explosively.

Operator training should emphasize the importance of responding to alarms. *They might be correct!* If operators ignore alarms, it may be because experience has taught them that alarms are unreliable. Are your alarms adequately maintained (see also Section 17.10)?

(c) A car on a pleasure ride in a leisure park developed a fault. The system was shut down automatically. The operator could not see the stranded car, assumed the trip was spurious, and restarted the ride with an override key. There were several collisions, and six people were injured. The company was fined, as the operator's training was described as "woefully inadequate" [8].

(d) An electron beam accelerator, used to irradiate cancer patients, broke down. After repair, the energy-level indicator showed 36 MeV when the energy-level selection keys were set for lower levels. The operators assumed that the needle was stuck at 36 MeV and carried on.

The needle was not stuck. The machine delivered 36 MeV whatever level was selected, and some patients got three to seven times more radiation than their doctors had prescribed. The beam was narrower than it should have been, and the radiation went deeper.

What went wrong? As well as the operators ignoring the warning reading, several other errors were made:

- The repairs had been botched though it is not clear whether the contract repairman did not know what to do or simply carried out a quick fix.
- The hospital physics service staff members were supposed to check, after repairs, that the energy level selected and the energy level indicated agreed. They did not check, as no one told them there had been a repair.
- The physics service was also supposed to carry out routine checks every day, but because few, if any, faults were found, the test interval was increased to a month. I doubt if anyone calculated the fractional dead time or hazard rate; the report does not say.
- A discrepancy between the energy level selected and the energy level indicated should trip the machine. However, the interlock had been easily bypassed by changing from automatic to manual control [9].

The incident was not simply the result of errors by the operating, repair, or physics staff members. They had been doing the wrong things for some time, but no one had noticed (or if they had noticed they did nothing). This is typical of human error accidents. Many people fail, many things are wrong, and it is unfair to put all the blame on the person who adds the last straw.

3.3.3 Ignorance of Hazards

This section presents a number of incidents that occurred because of ignorance of the most elementary properties of materials and equipment.

(a) A man who wanted some gasoline for cleaning decided to siphon it out of the tank of a company vehicle. He inserted a length of rubber tubing into the gasoline tank. Then, to fill the tubing and start the siphon, he held the hose against the suction nozzle of an industrial vacuum cleaner.

The gasoline caught fire. Two vehicles were destroyed and eleven damaged. This occurred in a branch of a large organization, not a small company.

(b) A new cooler was being pressure-tested using a water pump driven by compressed air. A plug blew out, injuring the two men on the job. It was then found that the pressure gauge had been fitted to the air supply instead of the cooler. The pressure had been taken far above the test pressure.

(c) An operator had to empty some tank trucks by gravity. He had been instructed to:

1. Open the valve on top of the tank.
2. Open the drain valve.
3. When the tank was empty, close the valve on top of the tank.

He had to climb onto the top of the tank twice. He therefore decided to close the vent before emptying the tank. To his surprise, the tank was sucked in.

(d) At one plant it was discovered that contractors' employees were using welding cylinders to inflate pneumatic tires. The welders' torches made a good fit on the tire valves.

3.3.4 Ignorance of Scientific Principles

The following incidents differ from those just described in that the operators, though generally competent, did not fully understand the scientific principles involved.

(a) A waste product had to be dissolved in methanol. The correct procedure was to put the waste in an empty vessel, box it up, evacuate it, break the vacuum with nitrogen, and add methanol. When the waste had dissolved, the solution was moved to another vessel, the dissolving vessel evacuated again, and the vacuum broken with nitrogen.

If this procedure is followed, a fire or explosion is impossible because air and methanol are never in the vessel together. However, to reduce the amount of work, the operators added the methanol as soon as the waste was in the vessel, without bothering to evacuate or add nitrogen. Inevitably, a fire occurred, and a man was injured. As often happens, the source of ignition was never identified.

It is easy to say that the fire occurred because the operators did not follow the rules. But why did they not follow the rules? Perhaps because they did not understand that if air and a flammable

vapor are mixed, an explosion may occur and that we cannot rely on removing all sources of ignition. To quote from an official report, on a similar incident, "we do feel that operators' level of awareness about hazards to which they may be exposing themselves has not increased at the same rate as has the level of personal responsibility which has been delegated to them" [3]. Also, the managers should have checked from time to time that the correct procedure was being followed.

(b) Welding had to take place near the roof of a storage tank that contained a volatile flammable liquid. There was a vent pipe on the roof of the tank, protected by a flame arrestor. Vapor coming out of this vent might have been ignited by the welding. The foreman therefore fitted a hose to the end of the vent pipe. The other end of the flex was placed on the ground so that the vapor now came out at ground level.

The liquid in the tank was soluble in water. As an additional precaution, the foreman therefore put the end of the flex in a drum of water. When the tank was emptied, the water first rose up the hose, and then the tank was sucked in. The tank, like most such tanks, was designed for a vacuum of 2½ in. water gauge only (0.1 psi or 0.6 kPa) and would collapse at a vacuum of about 6 in. water gauge (0.2 psi or 1.5 kPa).

If the tank had been filled instead of emptied, it might have burst, because it was designed to withstand a pressure of only 8 in. water gauge (0.3 psi or 2 kPa) and would burst at about three times this pressure. Whether it burst or not would have depended on the depth of water above the end of the flex.

This incident occurred because the foreman, though a man of great experience, did not understand how a lute works. He did not realize how fragile storage tanks usually are (see also Section 5.3).

(c) The emergency blowdown valves in a plant were hydraulically operated and were kept shut by oil under pressure. One day the valves opened, and the pressure in the plant blew off. It was then discovered that (unknown to the manager) the foremen, contrary to the instructions, were closing the oil supply valve "in case the pressure in the oil system failed"—a most unlikely occurrence and much less likely than the oil pressure leaking away from an isolated system.

Accidents that occurred because maintenance workers did not understand how things work or how they were constructed were described in Section 1.5.4.

3.3.5 Errors in Diagnosis

(a) The incident described in Section 3.2.8 is a good example of an error in diagnosis.

The operator correctly diagnosed that the rise in pressure in the reactor was due to a failure of the ethylene oxide to react. He decided that the temperature indicator might be reading high and that the temperature was therefore too low for reaction to start or that the reaction for some reason was sluggish to start and required a little more heat. He therefore raised the setting on the temperature interlock and allowed the temperature to rise.

His diagnosis, though wrong, was not absurd. However, having made a diagnosis, he developed a mind-set. That is, he stuck to it even though further evidence did not support it. The temperature rose, but the pressure did not fall. Instead of looking for another explanation or stopping the addition of ethylene oxide, he raised the temperature further and continued to do so until it reached 200°C instead of the usual 120°C. Only then did he realize that his diagnosis might be incorrect.

In developing a mind-set the operator was behaving like most of us. If we think we have found the solution to a problem, we become so committed to our theory that we close our eyes to evidence that does not support it. Specific training and practice in diagnostic skills may make it less likely that operators will make errors in diagnosis.

Duncan and co-workers [4] have described one method. Abnormal readings are marked on a drawing of the control panel (or a simulated screen). The operator is asked to diagnose the reasons for them and say what action he or she would take. The problems gradually get more difficult.

(b) The accident at Three Mile Island in 1979 provided another example of an error in diagnosis [5]. There were several indications that the level in the primary water circuit was low, but two instruments indicated a high level. The operators believed these two readings

and ignored the others. Their training had emphasized the hazard of too much water and the action to take but had not told them what to do if there was too little water in the system.

For more examples of accidents caused by human error and a discussion of responsibility, see Reference 6.

REFERENCES

1. J. Reason and K. Mycielska, *Absent Minded? The Psychology of Mental Lapses and Everyday Errors,* Prentice-Hall, Englewood Cliffs, N.J., 1982.
2. T. A. Kletz, *Chemical Engineering Progress,* Vol. 70, No. 7, Apr. 1974, p. 80.
3. *Annual Report of Her Majesty's Inspectors of Explosives for 1970,* Her Majesty's Stationery Office, London, 1971.
4. E. E. Marshall, et al., *The Chemical Engineer,* No. 365, Feb. 1981, p. 66.
5. T. A. Kletz, *Learning from Accidents,* 2nd edition, Butterworth-Heinemann, Oxford, UK, 1994, Chapter 11.
6. T. A. Kletz, *An Engineer's View of Human Error,* 2nd edition, Institution of Chemical Engineers, Rugby, UK, 1991.
7. *Lockout/Tagout Programs,* Safety Notice No. DOE/EH-0540, Office of Nuclear and Facility Safety, U.S. Dept. of Energy, Washington, D.C., 1996.
8. *Health and Safety at Work,* Nov. 1991, p. 10.
9. *Report on the Accident with the Linear Accelerator at the University Clinical Hospital of Zaragoza in December 1990,* Translation No. 91-11401 (8498e/813e), International Atomic Energy Agency, 1991.

Chapter 4

Labeling

> In my exploratory wanderings I would often ask what this or that pipe was conveying and at what pressure. Often enough there was no answer to my query, and a hole would have to be drilled to discover what the pipe contained.
>
> —A UK gas works in 1916, described by Norman Swindin, *Engineering Without Wheels*

Many incidents have occurred because equipment was not clearly labeled. Some of these incidents have already been described in the section on the identification of equipment under maintenance (Section 1.2).

Seeing that equipment is clearly and adequately labeled and checking from time to time to make sure that the labels are still there is a dull job, providing no opportunity to exercise our technical or intellectual skills. Nevertheless, it is as important as more demanding tasks are. One of the signs of good managers, foremen, operators, and designers is that they see to the dull jobs as well as those that are fun. If you want to judge a team, look at its labels as well as the technical problems it has solved.

4.1 LABELING OF EQUIPMENT

(a) Small leaks of carbon monoxide from the glands of a compressor were collected by a fan and discharged outside the building. A man working near the compressor was affected by carbon monoxide. It was then found that a damper in the fan delivery line was shut. There was no label or other indication to show when the damper was closed and when it was open.

In a similar incident, a furnace damper was closed in error. It was operated pneumatically. There was no indication on the control knob to show which was the open position and which was the closed position.

(b) On several occasions it has been found that the labels on fuses or switchgear and the labels on the equipment they supply do not agree. The wrong fuses have then been withdrawn. Regular surveys should be made to confirm that such labels are correct. Labels are a sort of protective equipment and, like all protective equipment, should be checked from time to time.

(c) Sample points are often unlabeled. As a result, the wrong material has often been sampled. This usually comes to light when the analysis results are received, but sometimes a hazard develops. For example, a new employee took a sample of butane instead of a higher boiling liquid. The sample was placed in a refrigerator, which became filled with vapor. Fortunately it did not ignite.

(d) Service lines are often not labeled. A fitter was asked to connect a steam supply at a gauge pressure of 200 psi (13 bar) to a process line to clear a choke. By mistake, he connected up a steam supply at a gauge pressure of 40 psi (3 bar). Neither supply was labeled, and the 40 psi supply was not fitted with a check valve. The process material came back into the steam supply line.

Later, the steam supply was used to disperse a small leak. Suddenly the steam caught fire.

It is good practice to use a different type of connector on each type of service point.

(e) Two tank trucks were parked near each other in a filling bay. They were labeled as shown in Figure 4-1. The filler said to the drivers, "Number eight is ready." He meant that No. 8 tank was ready, but the driver assumed that the tank attached to No. 8 tractor was ready. He got into No. 8 tractor and drove away. Tank No. 4 was still filling.

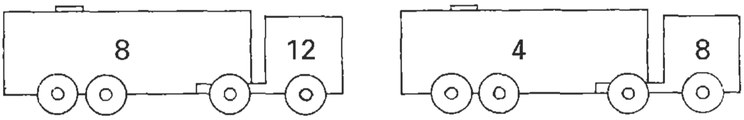


Figure 4-1. Arrangement of tank trailers and tractors.

Fortunately, the tank truck was fitted with a device to prevent it from departing when the filling hose was connected [1], and the driver was able to drive only a few yards.

If possible, tanks and tractors should be given entirely different sets of numbers.

(f) Nitrogen was supplied in tank cars that were also used for oxygen. Before filling the tank cars with oxygen, the filling connections were changed, and hinged boards on both sides of the tanker were folded down so that they read Oxygen instead of Nitrogen.

A tank car was fitted with nitrogen connections and labeled Nitrogen. Probably due to vibration, one of the hinged boards fell down so that it read Oxygen. The filling station staff therefore changed the connections and put oxygen in the tank car. Later, some nitrogen tank trucks were filled from the tank car, which was labeled Nitrogen on the other side—and supplied to a customer who wanted nitrogen. He off-loaded the oxygen into his plant, thinking it was nitrogen (Figure 4-2).

The mistake was found when the customer looked at his weighbridge figures and noticed that on arrival the tanker had weighed 3 tons more than usual. A check then showed that the plant nitrogen system contained 30% oxygen.

Analyze all nitrogen tankers before off-loading (see Section 12.3.4).

(g) A British Airways 747 had to make an emergency landing after sparks were seen coming out of an air conditioning vent. A motor bearing in a humidifier had failed, causing a short circuit, and the miniature circuit breakers (MCBs), which should have protected the circuit, had not done so. The reason: 25 amp circuit breakers had been installed instead of 2.5 amp ones. The fault current, estimated at 14 to 23 amps, was high enough to melt parts of the copper wire.

Figure 4-2. Arrangement of labels on tank cars. The Nitrogen label folds down to read Oxygen.

MCBs have been confused before. Different ratings look alike, and the part numbers are hard to read and are usually of the forms 123456-2.5 and 123456-25 [8].

(h) A lifting device had a design capacity of 15 tons, but in error it was fitted with a label showing 20 tons. As a result it was tested every year, for eight years, with a load of 1.5 times the indicated load, that is, with a load of 30 tons. This stressed the lifting device beyond its yield point though there was no visible effect. The ultimate load, at which the device would fail, was much higher, but it is bad practice to take equipment above its yield point [9].

(i) Notices should be visible. On more than one occasion someone has entered a section of a plant without the required protective clothing because the warning notice was shielded by a door normally propped open [10].

(j) A powder was conveyed in large plastic bags in a container fitted with a door. When someone started to open the door, the weight of the powder caused the bags to burst open, and he escaped injury only by leaping aside. The doors were intended to carry labels saying that it is dangerous to open them, but the one on this container was missing. However, a label is not sufficient; the door should have been locked.

4.2 LABELING OF INSTRUMENTS

(a) Plant pressures are usually transmitted from the plant to the control room by a pneumatic signal. This pneumatic signal, which is generated within the pressure-sensing element, usually has a gauge pressure in the range of 3 to 15 psi, covering the plant pressure from zero to maximum. For example, 3 to 15 psi (0.2 to 1 bar) might correspond to 0 to 1,200 psi plant pressure (0 to 80 bar).

The receiving gauge in the control room works on the transmitted pneumatic pressure, 15 psi giving full scale, but has its dial calibrated in terms of the plant pressure that it is indicating. The Bourdon tube of such a gauge is capable of withstanding only a limited amount of overpressure above 15 psi before it will burst. Furthermore, the material of the Bourdon tube is chosen for air and may be unsuitable for direct measurement of the process fluid pressure.

A pressure gauge of this sort with a scale reading up to 1,200 psi was installed directly in the plant. The plant gauge pressure was 800 psi, and the gauge was damaged.

Gauges of this type should have the maximum safe working pressure clearly marked in red letters on the face.

(b) A workman, who was pressure-testing some pipework with a hand-operated hydraulic pump, told his foreman that he could not get the gauge reading above 200 psi. The foreman told him to pump harder. He did and burst the pipeline.

The gauge he was using was calibrated in atmospheres and not psi. The word *ats* was in small letters, and in any case the workman did not know what it meant.

If more than one sort of unit is used in your plant for measuring pressure or any other property, then the units used should be marked on instruments in large, clear letters. You may use different colors for different units. Everyone should be aware of the differences between the units. However, it is better to avoid the use of different units.

(c) An extraordinary case of confusion between units occurred on a piece of equipment manufactured in Europe for a customer in England. The manufacturers were asked to measure all temperatures in °F and were told how to convert °C to °F.

A damper on the equipment was operated by a lever, whose position was indicated by a scale, calibrated in degrees of arc. These were converted to °F!

A medical journal reported that patients suffering from paracetamol poisoning should be nursed at 30°–40°. In the next issue, it said that this referred to the angle in bed, not the temperature [7].

(d) An operator was told to control the temperature of a reactor at 60°C. He set the set-point of the temperature controller at 60. The scale actually indicated 0%–100% of a temperature range of 0°–200°C, so the set-point was really 120°C. This caused a runaway reaction, which overpressured the vessel. Liquid was discharged and injured the operator [2].

(e) An error in testing made more probable by poor labeling is described in Section 3.2.4.

(f) Although digital instruments have many advantages, there are times when analog readings are better. One of the raw materials for a

batch reaction had to be weighed. The project team intended to install a weighing machine with a digital display, but an experienced operator asked for an analog scale instead because, he said, he was more likely to misread a figure than a position on a scale.

(g) A catalyst arrived in cylinders and was egged into the plant with nitrogen at a gauge pressure of 30 psi (2 bar). The gauge on the pressure regulator had two scales. The inner one, which was normally used, indicated 0–200 psig in divisions of 10 psi, so it was normally set at three divisions.

The regulator developed a fault and had to be changed. The gauge on the new one also had two scales. The inner one indicated 0–280 kg/cm^2 gauge (a kg/cm^2 is almost the same as a bar) in intervals of 10 kg/cm^2; the outer one indicated psig. The inner one thus looked like the inner scale on the old gauge, so the operators set the pointer at three divisions on it. Long before the pressure reached two divisions, corresponding to a gauge pressure of 20 kg/cm^2 or 300 psi, the cylinder burst. Figure 4-3 shows the results. The estimated bursting pressure was 215 psig (15 kg/cm^2 gauge) [11].

Figure 4-3. The result of pressurizing a cylinder to "two divisions" on a scale graduated in kg/cm^2 instead of psi. (*Photo courtesy of the Institution of Chemical Engineers.*)

4.3 LABELING OF CHEMICALS

4.3.1 Poor or Missing Labels

One incident is described in Section 2.8 (a). Several incidents have occurred because drums or bottles were unlabeled and people assumed that they contained the material usually handled at the plant. In one case, six drums of hypo (sodium hypochlorite) had to be added to a tank of water. Some of the drums were not labeled. One, which contained sulfuric acid, was added after some of the genuine hypo and chlorine was given off. The men adding the material in the drums were affected by the fumes.

In another case an unlabeled drum smelled like methylethylketone (MEK), so it was assumed to be MEK and was fed to the plant. Actually, it contained ethanol and a bit of MEK. Fortunately, the only result was a ruined batch.

Mononitro-o-xylene was manufactured by the nitration of o-xylene. An operator required some o-xylene to complete a series of batches. He found a tank labeled Xylene in another part of the plant and ran some of it into drums. It was then charged to the reactor. There was a violent reaction, a rupture disc blew, and about 600 gal of acid were discharged into the air through a vent pipe. Passers-by and schoolchildren were affected and needed first aid. The tank actually contained methanol and had contained it for eight months, but the label had not been changed though the engineering department had been asked to change it (note: if the vent pipe had discharged into a catchpot instead of the open air, the results of the runaway would have been trivial) [4].

Some nitric acid had to be flown from the U.S. to the UK. Several U.S. regulations were broken: the acid was packed in glass bottles instead of metal ones and was surrounded by sawdust instead of nonflammable material, and the boxes containing the bottles were not labeled as hazardous or marked This Side Up. The boxes were therefore loaded into the cargo aircraft on their sides, and the bottles leaked. Smoke entered the flight deck, and the crew decided to land, but while doing so the plane crashed, probably as the result of poor visibility on the flight deck, and the crew was killed. It is not clear why a common material of commerce had to be flown across the Atlantic [5].

Inspections showed that two cooling towers contained asbestos. Sticky warning labels were fixed to them. No maintenance work was carried out

on the towers until three years later. By this time the labels had been washed away. Nine members of the maintenance team removed filters from the towers without wearing protective equipment and may have been exposed to asbestos dust. Fortunately the asbestos was of a nonfriable type [12].

4.3.2 Similar Names Confused

Several incidents have occurred because similar names were confused. The famous case involving Nutrimaster (a food additive for animals) and Firemaster (a fire retardant) is well known. The two materials were supplied in similar bags. A bag of Firemaster, delivered instead of Nutrimaster, was mixed into animal feeding stuffs, causing an epidemic of illness among the farm animals. Farmers and their families were also affected [3].

In another case, a manufacturer of animal feedstuffs bought a starch additive from a Dutch company for incorporation in a milk substitute for calves. The Dutch company was out of stock, so it asked its UK affiliate company to supply the additive; the Dutch company quoted the product number. Unfortunately, the UK affiliate used this number to describe a different additive, which was highly toxic. As a result, 68,000 calves were affected, and 4,600 died. Chemicals (and equipment) should be ordered by name and not just by a catalog number [6].

A unit used small amounts of sodium sulfite and potassium sulfate. It was custom and practice to call these two chemicals simply sulfite and sulfate. During a busy period someone from another unit was asked to help and was told to prepare a batch of sulfate. The only sulfate he knew was aluminum sulfate, so he prepared a batch of it. Fortunately the error was spotted before the sulfate was used [13].

Other chemicals that have been confused, with resultant accident or injury, are:

1. Washing soda (sodium carbonate) and caustic soda (sodium hydroxide)
2. Sodium nitrite and sodium nitrate
3. Sodium hydrosulfide and sodium sulfide
4. Ice and dry ice (solid carbon dioxide)
5. Photographers' hypo (sodium thiosulfate solution) and ordinary hypo (sodium hypochlorite solution)

In the last case, a load of photographers' hypo was added to a tank containing the other sort of hypo. The two sorts of hypo reacted together, giving off fumes.

4.4 LABELS NOT UNDERSTOOD

Finally, even the best labels are of no use if they are not understood.

(a) The word *slops* means different things to different people. A tank truck collected a load of slops from a refinery. The driver did not realize that the slops were flammable. He took insufficient care, and they caught fire. He thought slops were dirty water.

(b) A demolition contractor was required to use air masks while demolishing an old tank. He obtained several cylinders of compressed air, painted gray. Finding that they would be insufficient, he sent a truck for another cylinder. The driver returned with a black cylinder. None of the men on the job, including the man in charge of the air masks, noticed the change or, if they did, attached any importance to it. When the new cylinder was brought into use, a welder's facepiece caught fire. Fortunately he pulled it off at once and was not injured.

The black cylinder had contained oxygen. All persons responsible for handling cylinders, particularly persons in charge of air masks, should be familiar with the color codes for cylinders.

REFERENCES

1. T. A. Kletz, *Loss Prevention,* Vol. 10, 1976, p. 151.
2. R. Fritz, *Safety Management* (South Africa), Jan. 1982, p. 27.
3. J. Egginton, *Bitter Harvest,* Secker and Warburg, London, 1980.
4. *Health and Safety at Work,* Vol. 8, No. 12, Dec. 1986, p. 8; and Vol. 9, No. 4, Apr. 1987, p. 37.
5. J. D. Lewis, *Hazardous Cargo Bulletin,* Feb. 1985, p. 44.
6. *Risk and Loss Management,* Vol. 2, No. 1, Jan. 1985, p. 21.
7. *Atom,* No. 400, Feb. 1990, p. 38.
8. *Bulletin 3/96,* Air Accident Investigation Branch, Defence Research Establishment, Farnborough, UK.

9. *Operating Experience Weekly Summary,* No. 97-13, Office of Nuclear and Facility Safety, U.S. Dept. of Energy, Washington, D.C., 1997, p. 5.
10. *Operating Experience Weekly Summary,* No. 97-20, Office of Nuclear and Facility Safety, U.S. Dept. of Energy, Washington, D.C., 1997, p. 7.
11. *Loss Prevention Bulletin,* No. 135, June 1997, p. 12.
12. *Operating Experience Weekly Summary,* No. 96-43, Office of Nuclear and Facility Safety, U.S. Dept. of Energy, Washington, D.C., 1996, p. 2.
13. C. Whetton, *Chemical Technology Europe,* Vol. 3, No. 4, July/Aug. 1996, p. 17.

Chapter 5

Storage Tanks

No item of equipment is involved in more accidents than the storage tank, probably because storage tanks are fragile and easily damaged by slight overpressure or vacuum. Fortunately, the majority of accidents involving tanks do not cause injury, but they do cause damage, loss of material, and interruption of production.

5.1 OVERFILLING

Most cases of overfilling are the result of lack of attention, wrong setting of valves, errors in level indicators, and so on (see Section 3.3.1 d). For this reason, many companies fit high-level alarms to storage tanks. However, overfilling has still occurred because the alarms were not tested regularly or the warnings were ignored (see Section 3.3.2 a).

Whether a high-level alarm is needed depends on the rate of filling and on the size of the batches being transferred into the receiving tank. If these are big enough to cause overfilling, a high-level alarm is desirable.

Spillages resulting from overfilling should be retained in tank dikes (bunds). But very often the drain valves on the dikes—installed so that rainwater can be removed—have been left open, and the spillage is lost to drain (see Section 5.5.2 c).

Drain valves should normally be locked shut. In addition, they should be inspected weekly to make sure they are closed and locked.

5.1.1 Alarms and Trips Can Make Overfilling More Likely

A high-level trip or alarm may actually *increase* the frequency of overfilling incidents if its limitations are not understood.

At one plant a tank was filled every evening with enough raw material for the following day. The operator watched the level. When the tank was full, he shut down the filling pump and closed the inlet valve. After several years, inevitably, one day he allowed his attention to wander, and the tank overflowed. It was then fitted with a high-level trip, which shut down the filling pump automatically.

To everyone's surprise the tank overflowed again a year later.

It had been assumed that the operator would continue to watch the level and that the trip would take over on the odd occasion when the operator failed to do so. Coincident failure of the trip was most unlikely. However, the operator no longer watched the level now that he was supplied with a trip. The manager knew that he was not doing so. But he decided that the trip was giving the operator more time for his other duties. The trip had the normal failure rate for such equipment, about once in two years, so another spillage after about two years was inevitable. A reliable operator had been replaced by a less reliable trip.

If a spillage about once in five years (or however often we think the operator will fail) cannot be accepted, then it is necessary to have two protective devices, one trip (or alarm) to act as a process controller and another to take over when the controller fails. It is unrealistic to expect an operator to watch a level when a trip (or alarm) is provided (see Section 14.7 a).

5.1.2 Overfilling Due to Change of Duty

On more than one occasion, tanks have overflowed because the contents were replaced by a liquid of lower specific gravity. The operators did not realize that the level indicator measured weight, not volume. For example, at one plant a tank that had contained gasoline (specific gravity 0.81) was used for storing pentane (specific gravity 0.69). The tank overflowed when the level indicator said it was only 85% full. The level indicator was a DP cell, which measures weight.

Another incident is described in Section 8.2 (b).

If the level indicator measures weight, it is good practice to fit a high-level alarm, which measures volume.

5.1.3 Overfilling by Gravity

Liquid is sometimes transferred from one tank to another by gravity. Overfilling has occurred when liquid flowed from a tall tank to a shorter one. On one occasion, an overflow occurred when liquid was transferred from one tank to another of the same height several hundred meters away. The operators did not realize that a slight slope in the ground was sufficient to cause the lower tank to overflow.

5.2 OVERPRESSURING

Most storage tanks are designed to withstand a gauge pressure of only 8 in. of water (0.3 psi or 2 kPa) and will burst at about three times this pressure. They are thus easily damaged. Most storage tanks are designed so they will burst at the roof/wall weld, thus avoiding any spillage, but older tanks may not be designed this way.

Tanks designed to fail at the roof/wall weld have failed at the base/wall weld because this weld was corroded or fatigued or because holding-down bolts were missing (Figure 5-1). Corrosion is most likely to occur in tanks containing a water layer or when spill absorbents have been placed around the base. Frequent emptying of a tank can cause fatigue failure of the base/wall weld. This can be prevented by leaving about 1 m depth of liquid in the tank when it is emptied [12].

5.2.1 Overpressuring with Liquid

Suppose a tank is designed to be filled at a rate of x m^3/hr. Many tanks, particularly those built some years ago, are provided with a vent big enough to pass x m^3/hr of air but not x m^3/hr of liquid. If the tank is overfilled, the delivery pump pressure will almost certainly be large enough to cause the tank to fail.

If the tank vent is not large enough to pass the liquid inlet rate, then the tank should be fitted with a hinged manhole cover or similar overflow device. Proprietary devices are available.

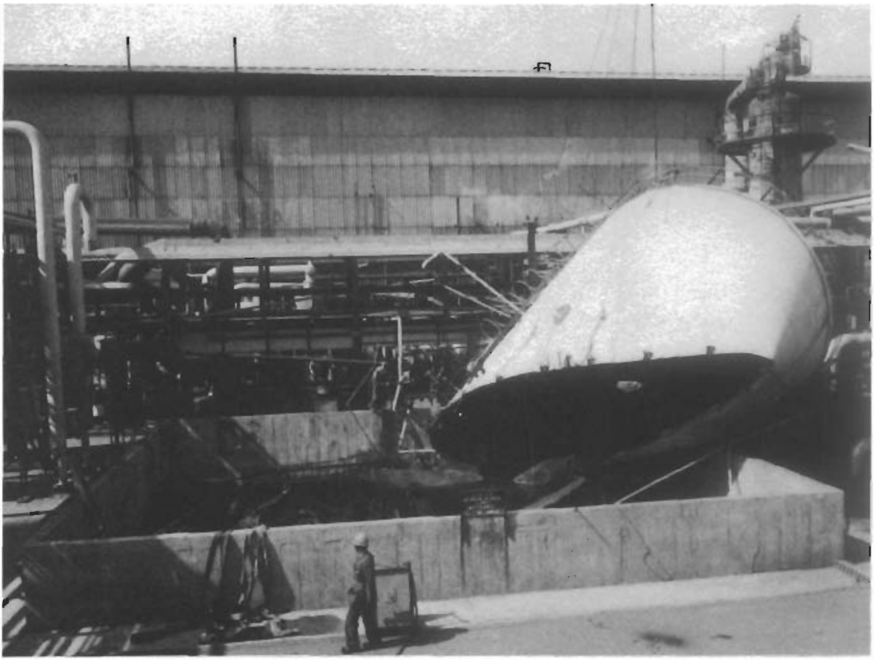


Figure 5-1. Corrosion and missing holding-down bolts caused this tank to fail at the base instead of the top.

This overflow device should be fitted to the roof near the wall. If it is fitted near the center of the roof, the height of liquid above the top of the walls may exceed 8 in., and the tank may be overpressured (see Figure 5-2a).

Similarly, if the vent is designed to pass liquid, it should be fitted near the edge of the roof, and its top should not be more than 8 in. above the tops of the walls. Vessels have been overpressured because their vent pipes were too long (see Figure 5-2b). Tanks in which hydrogen may be evolved should be fitted with a vent at the highest point as well as an overflow (see Section 16.2).

An 80 m^3 tank fiberglass-reinforced plastic acid tank was blown apart at the base as the result of overpressure. The vent had been slip-plated so the tank could be entered for inspection. The steel slip-plate was covered with a corrosion-resistant sheet of polytetrafluoroethylene. Afterward, when the slip-plate was removed, the sheet was left behind. This did not matter at the time, as the tank was also vented through an overflow line,

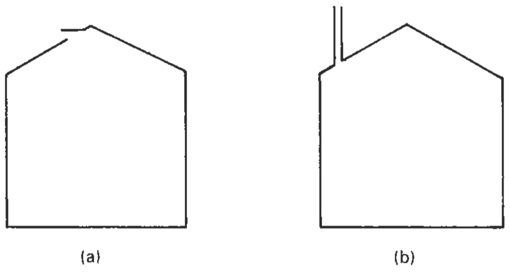


Figure 5-2. A tank may be overpressured if the vent or overflow is more than 8 in. above the tops of the walls.

which discharged into a sewer. A year later the sewer had to be maintained, so the overflow line was slip-plated to prevent acid from entering it during the overhaul. The operators were told to fill the tank slowly and watch the level. When they started to fill the tank, the reading on the level indicator rose rapidly, and the tank ruptured at the base. The level indicator was actually measuring the increasing pressure of the air in the tank as the liquid level rose and compressed the air in the tank [16].

5.2.2 Overpressuring With Gas or Vapor

This has usually occurred because those concerned did not realize that tanks are quite incapable of withstanding the pressure of the compressed air supply and that the vent may be too small to pass the inlet gas rate, as in the following two incidents:

(a) There was a choke on the exit line from a small tank. To try to clear the choke, the operator held a compressed air hose against the open end at the top of the level glass. The gauge pressure of the compressed air was 100 psi (7 bar), and the top of the tank was blown off (Figure 5-3).

(b) An old vessel, intended for use as a low-pressure storage tank, had been installed in a new position by a contractor who decided to pressure-test it. He could not find a water hose to match the hose connection on the vessel, and so he decided to use compressed air. The vessel ruptured.

Another incident in which a storage vessel was ruptured by compressed air is described in Section 2.2 (a).

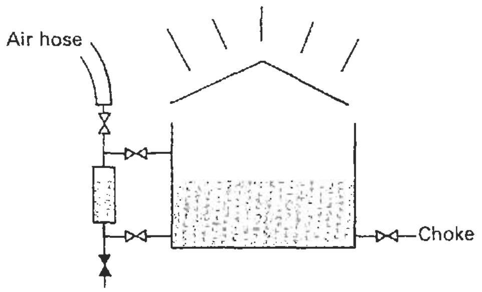


Figure 5-3. Tank top blown off by compressed air.

(c) On other occasions, tanks have been ruptured because the failure of a level controller allowed a gas stream to enter the tank (Figure 5-4). Pressure vessels have also been ruptured in this way (see Section 9.2.2 d).

The precautions necessary to prevent this from occurring are analyzed in detail in Reference 1.

(d) A storage tank for refrigerated butane was being brought back into service after maintenance. The tank was swept out with carbon

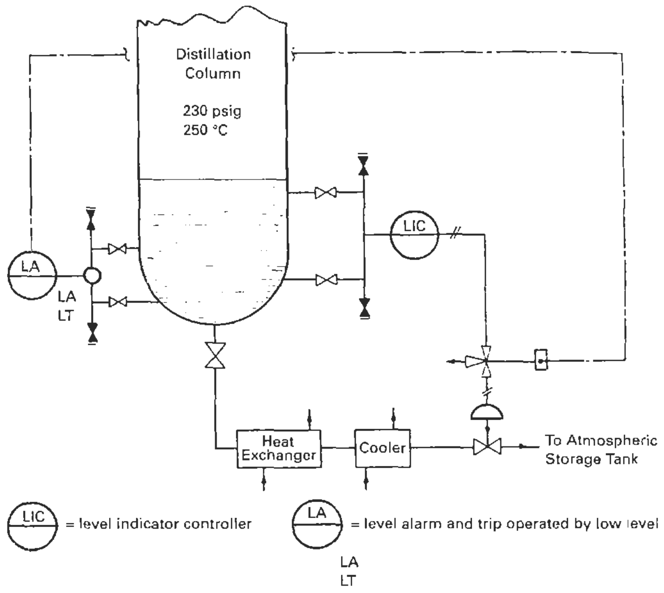


Figure 5-4. How failure of a level controller can overpressure a tank.

dioxide to remove the air, and the refrigerated butane was then added. As the tank cooled down, some of the butane vaporized, and a 2-in. vent was left open to prevent the pressure from rising. This was not large enough, so the operator opened a 6-in. vent. The pressure continued to rise. Both relief valves on the tank had been set at too high a pressure, and the butane addition rate was rather high. The tank floor became convex, and the holding-down fittings around the base were pulled out of the ground, but fortunately, the tank did not leak. The relief valves should have been set at a gauge pressure of 1.0 psi (0.07 bar)—the pressure in the tank probably reached 1.5–2 psi (0.1–0.14 bar) [13].

5.3 SUCKING IN

This is by far the most common way in which tanks are damaged. The ways in which it occurs are legion. Some are listed below. Sometimes it seems that operators show great ingenuity in devising new ways of sucking in tanks!

Many of the incidents occurred because operators did not realize how fragile tanks are. They can be overpressured easily but sucked in much more easily. While most tanks are designed to withstand a gauge pressure of 8 in. of water (0.3 psi or 2 kPa), they are designed to withstand a vacuum of only 2½ in. of water (0.1 psi or 0.6 kPa). This is the hydrostatic pressure at the bottom of a cup of tea.

Some incidents have occurred because operators did not understand how a vacuum works. See, for example, the incidents already described in Sections 3.3.3 (c) and 3.3.4 (b).

The following are some of the ways by which tanks have been sucked in. In some cases the vent was made ineffective. In others the vent was too small.

(a) Three vents were fitted with flame arrestors, which were not cleaned. After two years they choked. The flame arrestors were scheduled for regular cleaning (every six months), but this had been neglected due to pressure of work.

If you have flame arrestors on your tanks, are you sure they are necessary (see Section 6.2 g)?

(b) A loose blank was put on top of the vent to prevent fumes from coming out near a walkway.

(c) After a tank had been cleaned, a plastic bag was tied over the vent to keep dirt from getting in. It was a hot day. When a sudden shower cooled the tank, it collapsed.

(d) A tank was boxed up with some water inside. Rust formation used up some of the oxygen in the air (see Section 11.1 d).

(e) While a tank was being steamed, a sudden thunderstorm cooled it so quickly that air could not be drawn in fast enough. When steaming out a tank, a manhole should be opened. Estimates of the vent area required range from 10 in. diameter to 20 in. diameter.

On other occasions, vent lines have been isolated too soon after steaming stopped. Tanks that have been steamed may require several hours to cool.

(f) Cold liquid was added to a tank containing hot liquid.

(g) A pressure/vacuum valve (conservation vent) was assembled incorrectly—the pressure and vacuum pallets were interchanged. Valves should be designed so that this cannot occur (see Section 3.2.1).

(h) A pressure/vacuum valve was corroded by the contents of the tank.

(i) A larger pump was connected to the tank, and it was emptied more quickly than the air could get in through the vent.

(j) Before emptying a tank truck, the driver propped the manhole lid open. It fell shut.

(k) A tank was fitted with an overflow, which came down to ground level. There was no other vent. When the tank was overfilled, the contents siphoned out (Figure 5-5).

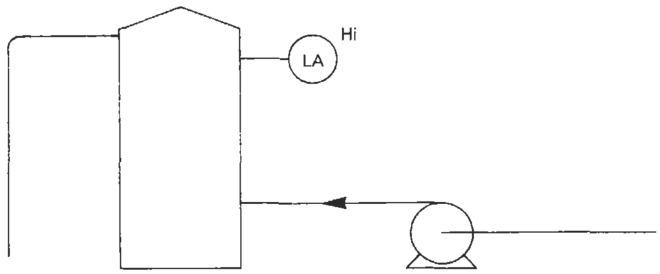


Figure 5-5. Overflow to ground level can cause a tank to collapse if there is no other vent.

The tank should have been fitted with a vent on its roof, as well as the liquid overflow.

(l) A vent was almost blocked by polymer (Figure 5-6). The liquid in the tank was inhibited to prevent polymerization, but the vapor that condensed on the roof was not inhibited. The vent was inspected regularly, but the polymer was not noticed.

Now a wooden rod is pushed through the vent to prove it is clear. (The other end of the rod should be enlarged so it cannot fall into the tank.)

(m) Water was added too quickly to a tank that had contained a solution of ammonia in water. To prevent the tank collapsing, the vent would have had to be 30 in. in diameter! This is impractical, so the water should therefore be added slowly through a restriction orifice or, better, a narrow bore pipe.

It is clear from these descriptions that we cannot prevent tanks from being sucked in by writing lists of do's and don'ts or by altering plant designs, except in a few cases (see items g and h). We can prevent these incidents only by increasing people's knowledge and understanding of the strength of storage tanks and of the way they work, particularly the way a vacuum works.

The need for such training is shown by the action taken following one of the incidents. Only the roof had been sucked in, and it was concave instead of convex. The engineer in charge decided to blow the tank back to the correct shape by water pressure. He gave instructions for this to be done. A few hours later he went to see how the job was progressing. He found that the tank had been filled with water and that a hand-operated

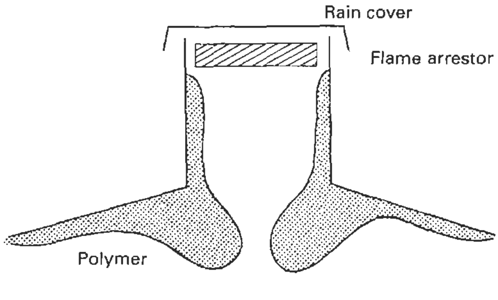


Figure 5-6. Vent almost blocked by polymer.

hydraulic pump, normally used for pressure-testing pipework, was being connected to the tank. He had it removed, and he replaced the vent with a vertical pipe, 1 m long. He dribbled water into the pipe from a hose, and as he did so the tank was restored to its original shape (Figure 5-7) to the amazement of onlookers. The static pressure of the water in the pipe was sufficient.

5.4 EXPLOSIONS

Explosions in the vapor spaces of fixed-roof storage tanks have been numerous. One estimate puts the probability of an explosion at about once in 1,000 years per tank, based on historical records. According to a 1997 report, 25–30 storage tank explosions occur per year in Canada alone [17]. The reason for the large number of explosions is that explosive mixtures are present in the vapor spaces of many storage tanks. It is almost impossible to be certain that a source of ignition will never turn up, particularly if the liquid in the tank has a low conductivity so that static charges can accumulate on the liquid. For this reason, many companies do not allow explosive mixtures to form. They insist that fixed-roof storage tanks containing hydrocarbons above their flash points are blanketed with nitrogen (see Section 5.6.3). Other companies insist that such hydrocarbons are stored only in floating-roof tanks.

Nonhydrocarbons usually have a higher conductivity than hydrocarbons. (Nonhydrocarbons with a symmetrical molecule, such as diethyl ether and carbon disulfide, have a low conductivity.) Charges of static electricity can rapidly drain away to earth (provided the equipment is grounded), and the risk of ignition is much lower. Many companies therefore store these materials in fixed-roof tanks without nitrogen blanketing [2].

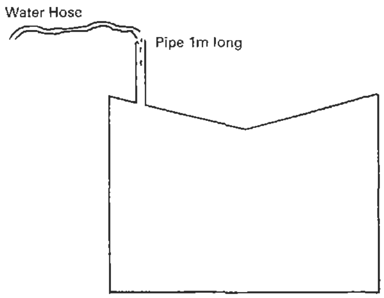


Figure 5-7. Method of restoring a tank with a concave roof to its original shape.

External sources of ignition, such as lightning (Figure 5-8) or welding near an open vent, can also trigger a tank explosion. Sample and dip holes and other openings should be kept closed or protected by flame arrestors. These are liable to choke and need regular inspection (see Sections 5.3 a, 6.2 g, and 14.2.4).

5.4.1 A Typical Tank Explosion

A large tank blew up 40 minutes after the start of a blending operation in which one grade of naphtha was being added to another. The fire was soon put out, and the naphtha was moved to another tank. The next day, blending was resumed; 40 minutes later, another explosion occurred.

The tanks were not nitrogen-blanketed, and there was an explosive mixture of naphtha vapor and air above the liquid in the tanks. The source of ignition was static electricity. The pumping rate was rather high so that the naphtha flowing through the pump and lines acquired a charge. A spark passed between the liquid in the tank and the roof or walls of the tank, igniting the vapor-air mixture.

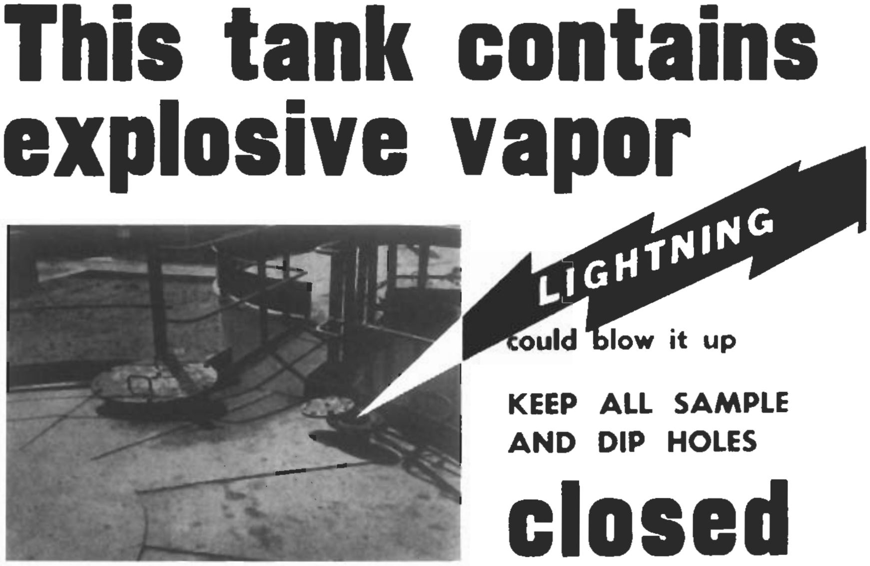


Figure 5-8.

These explosions led to an extensive series of investigations into the formation of static electricity [3].

There are several ways of preventing similar explosions:

1. Use nitrogen blanketing or floating-roof tanks.
2. Use antistatic additives; they increase the conductivity of the liquid so that charges can drain away rapidly to earth (provided equipment is grounded). However, make sure that the additives do not deposit on catalysts or interfere with chemical operations in other ways.
3. Minimize the formation of static electricity by keeping pumping rates low (less than 3 m/s for pure liquids but less than 1 m/s if water is present) and avoiding splash filling. Filters and other restrictions should be followed by a long length of straight line to allow charges to decay.

It is difficult to feel confident that No. 3 can always be achieved, and therefore No. 1 or No. 2 is recommended.

For more information on static electricity, see Chapter 15.

5.4.2 Some Unusual Tank Explosions

(a) A new tank was being filled with water for hydrostatic testing when an explosion occurred. Two welders who were working on the roof. finishing the handrails, were injured, fortunately not seriously.

The tank had been filled with water through a pipeline that had previously contained gasoline. A few liters left in the line were flushed into the tank by the water and floated on top of it. The vapor was ignited by the welders.

No one should be allowed to go onto the roof of a tank while it is being filled with water for testing. One of the reasons for filling it with water is to make sure that the tank and its foundations are strong enough. If we were sure they were, we would not need to test. People should be kept out of the way, in case they are not.

(b) During the construction of a new tank, the contractors decided to connect the nitrogen line to the tank. They knew better, they said, than to connect the process lines without authority. But nitrogen was inert and therefore safe.

The new tank and an existing one were designed to be on balance with each other to save nitrogen (Figure 5-9), but the contractors did not understand this. The valve to the new tank was closed but leaking. Nitrogen and methanol vapor entered the tank, and the vapor was ignited by a welder who was completing the inlet line to the tank. The roof was blown right off. By great good fortune, it landed on a patch of empty ground just big enough to contain it (Figure 5-10).

(c) The roof of an old gasoline tank had to be repaired. The tank was steamed out and cleaned, and tests with a combustible gas detector showed that no flammable gas or vapor was present. A welder was therefore allowed to start work. Soon afterward, a small flash of flame singed his hair.

The roof was made from plates, which overlapped each other by about 4 in. and which were welded together on the top side only—an old method of construction that is not now used (Figure 5-11). It is believed that some gasoline entered the space between the plates and became trapped by rust and scale. The heat from the welding vaporized the gasoline, and it blew out of the molten weld. At the time, the suggestion was made that the tank should be filled with water, but this cannot be done without risking overpressuring the tank (see Section 5.2.1).

(d) Some welding had to take place at the top of a 38-m^3 tank containing about 10 m^3 of hydrocarbons and water. Instead of emptying the tank and sweeping out the remaining vapor with steam or nitrogen—the usual procedure—the people in charge tested the inside of the tank, just below a roof opening, with a combustible gas detector. As they got a zero reading, they decided to go ahead with the welding. The roof was blown off the tank, landing 30 m away, killing one man and injuring another.

It is believed that a hot speck, loosened by the welding, fell off the inside of the roof and ignited a flammable mixture that was present near the surface of the liquid [18]. Tests have shown that the atmosphere in a tank can take a long time to reach equilibrium when the liquid level is low.

As stated in Section 1.3.1, large vessels should be tested in several places.

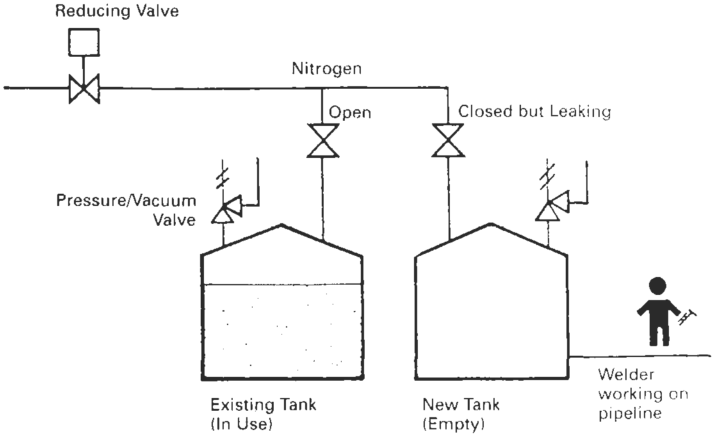


Figure 5-9. If tanks are on balance, the nitrogen entering one tank is inevitably mixed with vapor.

Figure 5-10. When an explosion occurred in a tank, the roof landed on an area just big enough to contain it.

Figure 5-11. An old method of tank construction allows liquid to enter the gap between the plates.

(e) During the manufacture of zinc, metallic impurities are removed by addition of zinc slurry or powder to an acidic solution of zinc salts in a number of tanks fitted with vents, overflows, and extract fans. Hydrogen is produced and has to be removed. In a new plant, there was no inerting and the so-called "basis of safety" (really a basis of danger) was to operate with the hydrogen concentration either below the lower flammable limit (4%) or above the upper flammable limit (75%) and to pass rapidly between the two, as follows (see Figure 5-12):

- When zinc was added to a tank, the extract fans were operated at full rate with the vent closed. No air could be sucked in, and the concentration of hydrogen rose rapidly above the upper flammable limit (75%).
- The fan speed was then lowered.
- When the rate of production of hydrogen fell, the fans were again switched to full rate, this time with the vent open. Air was sucked in, and the concentration of hydrogen fell rapidly below the lower flammable limit.

After three months of operation, an explosion occurred in a 400 m^3 tank, which fortunately was fitted with explosion relief. Three weeks later another explosion blew the roof off another tank, and the Australian Department of Mines ordered the closure of the plant.

Stage	Vent	Fan speed	Objective
Start	Shut	High	Remove air and get above UEL quickly
Run	Shut	Low	Stay above UEL
Near end	Open	High	Suck in air and get below LEL quickly

Results:
After three months of operation: mild explosion; vent panel lifted.
Three weeks later: another explosion; roof blown off tank.

Modifications:
Tanks inerted except for a few, which were sparged with air to keep below the lower explosive limit.

UEL = upper explosive limit
LEL = lower explosive limit

(Reproduced with permission of the American Institute of Chemical Engineers. Copyright © 1995 AIChE. All rights reserved.)

Figure 5-12. An attempt to avoid explosions by passing quickly through the explosive range was not successful.

The source of ignition was never found, but a report [19] on the explosion lists six possible causes, thus confirming the view—well known to everyone except those who designed and operated the plant—that sources of ignition are so numerous that we can never be sure they will not turn up even though we do what we can to remove known sources. Flammable mixtures should not be deliberately allowed to form except under rigidly defined circumstances where the chance of an occasional ignition is accepted. This is particularly true where hydrogen is handled, as it is more easily ignited than most other gases or vapors.

The plant was restarted after 23 days. Most of the tanks are now blanketed with nitrogen, but a few, which were difficult to blanket, are fitted with an air sparge system designed to keep the hydrogen concentration well below 25% of the lower flammable limit.

(f) Paper mills use large quantities of water, and the water is usually recycled. Buffer storage is needed, and at one paper mill, it took the form of a 740-m^3 tank. Experience showed that this was insufficient, and another tank of the same size was installed alongside. To simplify installation it was not connected in parallel with the original tank but on balance with it, as shown in Figure 5-13. A week after the new tank was brought into use, welders were completing the handrails on the roof when an explosion occurred in the tank. Two welders were killed, and the tank was blown 20 m into the air, landing on a nearby building.

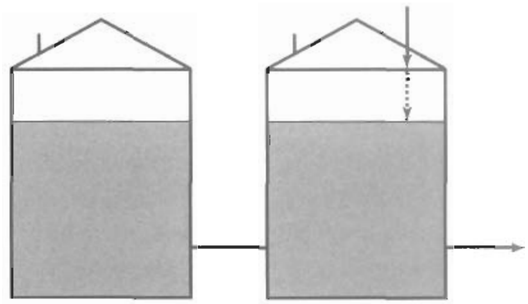


Figure 5-13. Extra buffer storage for water was provided by installing a second tank on balance with the first one. Lack of aeration allowed hydrogen-forming bacteria to grow, and an explosion occurred. *(Reproduced with permission of the American Institute of Chemical Engineers. Copyright © 1995 AIChE. All rights reserved.)*

Investigation showed that the explosion was due to hydrogen formed by anaerobic bacteria. In the original tank the splashing of the inlet liquor aerated the water and prevented anaerobic conditions. This did not apply in the new tank [20].

The incident shows once again how a simple modification, in this case adding liquid to the bottom of a tank instead of the top, can produce an unforeseen hazard. In the oil and chemical industries we are taught to add liquid to the bottom of a tank, not the top, to prevent splashing, the production of mist, and the generation of static electricity (see Section 5.4.1). No rule is universal.

Hydrogen produced by corrosion has also turned up in some unexpected places (see Section 16.2).

As mentioned in Section 1.1.4, bacterial action on river water can also produce methane.

Fires and explosions that occurred while repairing or demolishing storage tanks containing traces of heavy oil are described in Section 12.4.1 and an explosion of a different type is described at the end of Section 1.1.4.

5.4.3 An Explosion in an Old Pressure Vessel Used as a Storage Tank

Sometimes old pressure vessels are used as storage tanks. It would seem that by using a stronger vessel than is necessary we achieve greater safety. But this may not be the case, as if the vessel fails, it will do so more spectacularly (see Section 2.2 a).

A tank truck hit a pipeline leading to a group of tanks. The pipeline went over the top of the dike wall, and it broke off inside the dike. The engine of the truck ignited the spillage, starting a dike fire, which damaged or destroyed 21 tanks and 5 tank trucks.

An old 100-m^3 pressure vessel, a vertical cylinder, designed for a gauge pressure of 5 psi (0.3 bar), was being used to store, at atmospheric pressure, a liquid of flash point 40°C. The fire heated the vessel to above 40°C and ignited the vapor coming out of the vent; the fire flashed back into the tank, where an explosion occurred. The vessel burst at the bottom seam, and the entire vessel, except for the base, and contents went into orbit like a rocket [4].

If the liquid had been stored in an ordinary low-pressure storage tank with a weak seam roof, then the roof would have come off, and the burning liquid would have been retained in the rest of the tank.

The incident also shows the importance of cooling, with water, all tanks or vessels exposed to fire. It is particularly important to cool vessels. They fail more catastrophically, either by internal explosion or because the rise in temperature weakens the metal (see Section 8.1).

Another tank explosion is described in Section 16.2 (a).

5.5 FLOATING-ROOF TANKS

This section describes some incidents that could only have occurred on floating-roof tanks.

5.5.1 How to Sink the Roof

A choke occurred in the flexible pipe that drained the roof of a floating-roof tank. It was decided to drain rainwater off the roof with a hose. To prime the hose and establish a siphon, the hose was connected to the water supply. It was intended to open the valve on the water supply for just long enough to fill the hose. This valve would then be closed and the drain valve opened (Figure 5-14). However, the water valve was opened in error and left open, with the drain valve shut. Water flowed onto the floating roof and it sank in 30 minutes (see also Section 18.8).

Temporary modifications should be examined with the same thoroughness as permanent ones (see Section 2.4).

5.5.2 Fires and Explosions

(a) Most fires on floating-roof tanks are small rim fires caused by vapor leaking through the seals. The source of ignition is often atmospheric electricity. It can be eliminated as a source of ignition

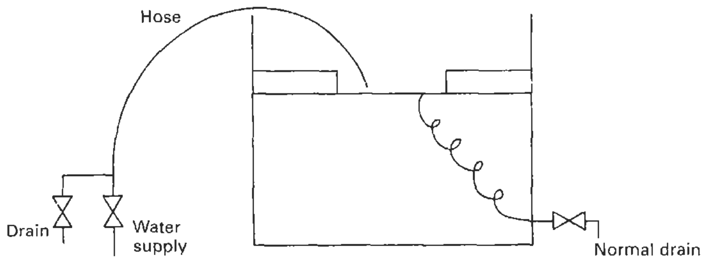


Figure 5-14. How to sink the roof of a floating-roof tank.

by fitting shunts—strips of metal—about every meter or so around the rim to ground the roof to the tank walls.

Many rim fires have been extinguished by a worker using a handheld fire extinguisher. However, in 1979, a rim fire had just been extinguished when a pontoon compartment exploded, killing a fireman. It is believed that there was a hole in the pontoon and some of the liquid in the tank leaked into it.

Workers should not go onto floating-roof tanks to extinguish rim fires [5]. If fixed fire-fighting equipment is not provided, foam should be supplied from a monitor.

(b) The roof of a floating-roof tank had to be replaced. The tank was emptied, purged with nitrogen, and steamed for six days. Each of the float chambers was steamed for four hours. Rust and sludge were removed from the tank. Demolition of the roof was then started.

Fourteen days later a small fire occurred. About a gallon of gasoline came out of one of the hollow legs that support the roof when it is off-float and was ignited by a spark. The fire was put out with dry powder.

It is believed that the bottom of the hollow leg was blocked with sludge and that, as cutting took place near the leg, the leg moved and disturbed the sludge (Figure 5-15).

Before welding or burning is permitted on floating-roof tanks, the legs should be flushed with water from the top. On some tanks, the bottoms of the legs are sealed. Holes should be drilled in them so they can be flushed through.

(c) Sometimes a floating roof is inside a fixed-roof tank. In many cases, this will reduce the concentration of vapor in the vapor space below the explosive limit. But in other cases it can increase the hazard, because vapor that was previously too rich to explode is brought into the explosive range.

A serious fire that started in a tank filled with an internal floating roof is described in Reference [6].

As a result of a late change in design, the level at which a floating roof came off-float had been raised, but this was not marked on the drawings that were given to the operators. As a result, without intending to, they took the roof off-float. The pressure/vacuum

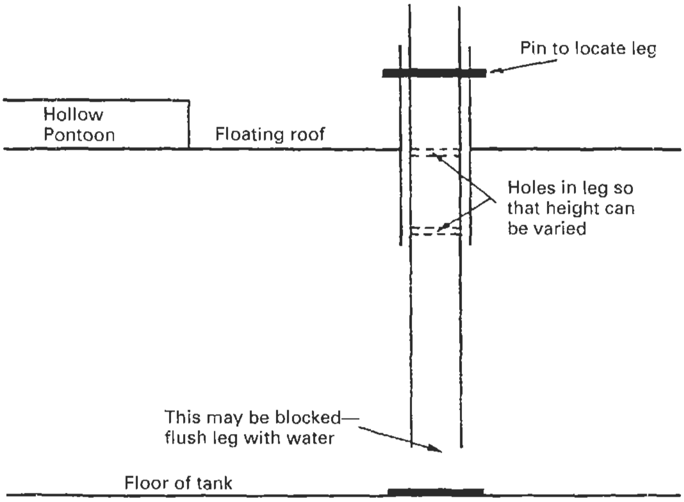


Figure 5-15. Oil trapped in the leg of a floating-roof tank caught fire during demolition.

valve (conservation vent) opened, allowing air to be sucked into the space beneath the floating roof.

When the tank was refilled with warm crude oil at 37°C, vapor was pushed out into the space above the floating roof and then out into the atmosphere through vents on the fixed-roof tank (Figure 5-16). This vapor was ignited at a boiler house some distance away.

The fire flashed back to the storage tank, and the vapor burned as it came out of the vents. Pumping was therefore stopped. Vapor no longer came out of the vents, air got in, and a mild explosion occurred inside the fixed-roof tank. This forced the floating roof down like a piston, and some of the crude oil came up through the seal past the side of the floating roof and out of the vents on the fixed-roof tank. This oil caught fire, causing a number of pipeline joints to fail, and this caused further oil leakages. One small tank burst; fortunately, it had a weak seam roof. More than 50 fire appliances and 200 firemen attended, and the fire was under control in a few hours.

The water level outside the dike rose because the dike drain valve had been left open, and the dike wall was damaged by the

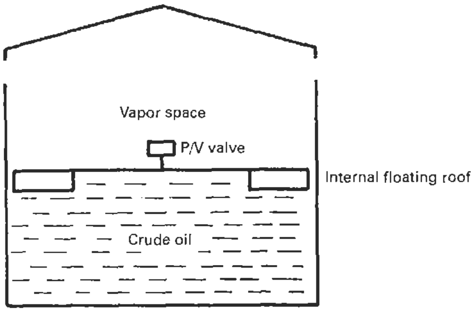


Figure 5-16. Tank with internal floating roof.

fire-fighting operations. The firemen pumped some of the water into another dike, but it ran out because the drain valve on this dike had also been left open.

An overhead power cable was damaged by the fire and fell down, giving someone an electric shock. The refinery staff members therefore isolated the power to all the cables in the area. Unfortunately they did not tell the firemen what they were going to do. Some electrically driven pumps that were pumping away some of the excess water stopped, and the water level rose even further. Despite a foam cover, oil floating on top of the water was ignited by a fire engine that was parked in the water. The fire spread rapidly for 150 m. Eight firemen were killed and two seriously injured. A naphtha tank ruptured, causing a further spread of the fire, and it took 15 hours to bring it under control.

The main lessons from this incident are:

1. Keep plant modifications under control and keep drawings up to date (see Chapter 2).
2. Do not take floating-roof tanks off-float except when they are being emptied for repair.
3. Keep dike drain valves locked shut. Check regularly to make sure they are shut.
4. Plan now how to get rid of fire-fighting water. If the drains will not take it, it will have to be pumped away.
5. During a fire, keep in close touch with the firemen and tell them what you propose to do.

(d) Roof cracks led to an extensive fire on a large (94,000 m^3) tank containing crude oil. The cracking was due to fatigue, the result of movement of the roof in high winds, and a repair program was in hand. A few days before the fire, oil was seen seeping from several cracks, up to 11 in. long, on the single-skin section of the floating roof, but the tank was kept in use, and no attempt was made to remove the oil. The oil was ignited, it is believed, by hot particles of carbon dislodged from a flarestack 108 m away and 76 m high, the same height as the tank. The fire caused the leaks to increase, and the tank was severely damaged. Six firemen were injured when a release of oil into the dike caused the fire to escalate. The fire lasted 36 hours. 25,000 tons of oil were burned, and neighboring tanks, 60 m away, were damaged. The insulation on one of these tanks caught fire, and the tank was sucked in, but the precise mechanism was not clear [9, 10].

The release of oil into the dike was due to boilover, that is, production of steam from the fire-fighting foam by the hot oil. As the steam leaves the tank, it brings oil with it. Boilover usually occurs when the heat from the burning oil reaches the water layer at the bottom of the tank, but in this case it occurred earlier than usual when the heat reached pockets of water trapped on the sunken roof [14].

Most large floating roofs are made from a single layer of steel, except around the edges, where there are hollow pontoons to give the roof its buoyancy. The single layer of steel is liable to crack, and any spillage should be covered with foam and then removed as soon as possible. Double-deck roofs are obviously safer but much more expensive [14].

5.6 MISCELLANEOUS INCIDENTS

5.6.1 A Tank Rises Out of the Ground

A tank was installed in a concrete-lined pit. The pit was then filled with sand, and a layer of concrete 6 in. thick was put over the top. Water accumulated in the pit, and the buoyancy of the tank was sufficient to break the holding-down bolts and push it through the concrete covering.

A sump and pump had been provided for the removal of water. But either the pump-out line had become blocked or pumping had not been carried out regularly [7].

Underground tanks are not recommended for plant areas. They cannot be inspected for external corrosion, and the ground is often contaminated with corrosive chemicals.

5.6.2 Foundation Problems

Part of the sand foundation beneath a 12-year-old tank subsided. Water collected in the space that was left and caused corrosion. This was not detected because the insulation on the tank came right down to the ground.

When the corrosion had reduced the wall thickness from 6 mm to 2 mm, the floor of the tank collapsed along a length of 2.5 m, and 30,000 m^3 of hot fuel oil came out. Most of it was collected in the dike. However, some leaked into other dikes through rabbit holes in the earth walls.

All storage tanks should be scheduled for inspection every few years. And on insulated tanks the insulation should finish 200 mm above the base so that checks can be made for corrosion.

Tanks containing liquefied gases that are kept liquid by refrigeration sometimes have electric heaters beneath their bases to prevent freezing of the ground. When such a heater on a liquefied propylene tank failed, the tank became distorted and leaked—but fortunately, the leak did not ignite. Failure of the heater should activate an alarm. As stated in Section 5.2, frequent complete emptying of a tank can weaken the base/wall weld.

5.6.3 Nitrogen Blanketing

Section 5.4.1 discussed the need for nitrogen blanketing. However, if it is to be effective, it must be designed and operated correctly.

Incorrect design

On one group of tanks the reducing valve on the nitrogen supply was installed at ground level (Figure 5-17). Hydrocarbon vapor condensed in the vertical section of the line and effectively isolated the tank from the nitrogen blanketing.

The reducing valve should have been installed at roof height. Check your tanks—there may be more like this one.

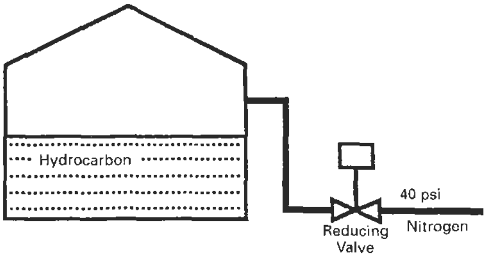


Figure 5-17. Incorrect installation of nitrogen blanketing.

Incorrect operation

An explosion and fire occurred on a fixed-roof tank that was supposed to be blanketed with nitrogen. After the explosion, it was found that the nitrogen supply had been isolated. Six months before the explosion the manager had personally checked that the nitrogen blanketing was in operation. But no later check had been carried out [8].

All safety equipment and systems should be scheduled for regular inspection and test. Nitrogen blanketing systems should be inspected at least weekly. It is not sufficient to check that the nitrogen is open to the tank. The atmosphere in the tank should be tested with a portable oxygen analyzer to make sure that the oxygen concentration is below 5%.

Large tanks (say, over 1,000 m^3) blanketed with nitrogen should be fitted with low-pressure alarms to give immediate warning of the loss of nitrogen blanketing.

5.6.4 Brittle Failure

On several occasions a tank has split open rapidly from top to bottom, as if it were fitted with a zipper and someone pulled it. An official report [15] describes one incident in detail:

The tank, which was nearly full, contained 15,000 m^3 of diesel oil, which surged out of the failed tank like a tsunami, washing over the dike walls. About 3,000 m^3 escaped from the site into a river that supplied drinking water for neighboring towns, disrupting supplies for a week. Fortunately no one was killed.

The collapse was due to a brittle failure that started at a flaw in the shell about 2.4 m above the base. The fault had been there since the tank

was built more than 40 years earlier, and the combination of a full tank and a low temperature triggered the collapse. For most of the 40 years, the tank had been used for the storage of a fuel oil that had to be kept warm; the high temperature prevented a brittle failure. However, two years before the collapse, the tank had been dismantled, re-erected on a new site, and used for the storage of diesel oil at ambient temperature.

The flaw was close to the edge of a plate, and if the contractor that moved the tank had cut it up along the welds—the usual practice—some or all of the flaw might have been removed. However, the tank was cut up close to the welds but away from them. The flaw was obscured by rust and residue and could not be seen.

The owner and contractor are strongly criticized in the report for not complying with the relevant American Petroleum Institute codes. They did not radiograph all T-joints (the flaw was close to a T-joint and would have been detected), and they did not realize that the grade of steel used and the quality of the original welding were not up to modern standards. The comments about the engineers in charge are similar to those made in the Flixborough report (see Section 2.4 a): their lack of qualifications "does not necessarily affect their ability to perform many aspects of a project engineer's job. However, when tough technical issues arise, such as whether to accept defective welds, a stronger technical background is required. If help on such matters was available . . ., there is no evidence that . . . utilized it . . ." (p. 69 of the report).

The summing up of the report reminds us of similar comments made about many serious accidents in other industries: the company (a large independent oil refiner) "failed to take any active or effective role in controlling its contractors or establish any procedures which might lead to a quality job. It was a passive consumer of the worst kind—apathetic as to potential problems, ignorant of actual events, unwilling to take any engaged role. Its employees were both institutionally and often personally unable to respond in any other way. Both the details and the big picture equally escaped [the company's] attention. Compared against the applicable standards, its industry peers, or even common sense [the company's] conduct and procedures can only be considered grossly negligent. The structural collapse . . . can be directly traced to the supervisory bankruptcy at [the company]" (p. 79 of the report).

The report also includes a list of other similar tank collapses: six in the U.S. in the period 1978–1986 (p. 102). A similar incident involving a liquefied propane tank occurred in Qatar in 1977 (see Section 8.1.5).

5.7 FRP TANKS

Tanks made from fiberglass-reinforced plastic are being increasingly used, but a number of failures have occurred. In the United Kingdom 30 catastrophic failures are known to have occurred during the period 1973–1980, and a 1996 report shows that they seem to have been continuing at a similar rate [21]. The following typify the catastrophic failures that have occurred [11]:

(a) A 50 m^3 tank made from bolted sections failed because the bolts holding the steel reinforcements together were overstressed. The contents—liquid clay—pushed over a wall and ran into the street.

(b) Ninety cubic meters of sulfuric acid was spilled when a tank failed as the result of stress corrosion cracking. It had not been inspected regularly, and the company was not aware that acid can affect FRP tanks. The failure was so sudden that part of the dike wall was washed away.

(c) Another tank, used to store a hot, acidic liquid, failed because it was heated above its design temperature and damaged when digging out residues. Again, it had not been inspected regularly, and the company was not aware of the effects of acid.

(d) Forty-five cubic meters of 10% caustic soda solution was spilled when the end came off a horizontal cylindrical tank. The polypropylene lining was leaking, and the caustic soda attacked the FRP.

(e) Three hundred fifty cubic meters of hot water was spilled and knocked over a wall when a tank failed at a brewery. The grade of FRP used was unsuitable, and the tank had never been inspected during the three years it had been in use. Another failure of a plastic hot water tank is described in Section 12.2.

(f) Thirty tons of acid were spilled when a tank failed. A weld was below standard, and stress corrosion cracking occurred. There had been no regular inspections.

(g) An internal lining failed as the result of bending stresses, and the acidic contents attacked the FRP. Cracks in the tank had been noticed and repaired, but no one investigated why they had occurred. Finally, the tank failed catastrophically, and the contents knocked over a wall.

(h) An FRP tank leaked near a manway after only 18 months in service. The wall thickness was too low, the welding was substandard, and this poor construction was not detected during inspection. The tank failed the first time it was filled to 85% capacity, and this suggests that it was never tested properly after installation [21].

These incidents show that, to prevent failures of FRP tanks, we should:

1. Use equipment designed for the conditions of use.
2. Know the limitations of the equipment.
3. Inspect regularly.
4. Not repair faults and carry on until their cause is known.

These rules, of course, apply generally, but they are particularly applicable to FRP tanks.

REFERENCES

1. T. A. Kletz and H. G. Lawley, in A. E. Green (editor), *High Risk Safety Technology,* Wiley, Chichester, UK, 1982, Chapter 2.1.
2. T. A. Kletz, "Hard Analysis—A Quantitative Approach to Safety," Symposium Series No. 34, Institution of Chemical Engineers, 1971, p. 75.
3. A. Klinkenberg and J. L. van der Minne, *Electrostatics in the Petroleum Industry,* Elsevier, Amsterdam, 1958.
4. *Loss Prevention,* Vol. 7, 1972, p. 119; and Manufacturing Chemists Association, *Case History No. 1887,* Washington, D.C., 1972.
5. D. K. McKibben, "Safe Design of Atmospheric Pressure Vessels," Paper presented at Seminar on Prevention of Fires and Explosions in the Hydrocarbon Industries, Institute of Gas Technology, Chicago, June 21–26, 1982.
6. Press release issued by the City of Philadelphia Office of the City Representatives, Dec. 12, 1975.
7. *Petroleum Review,* Oct. 1974, p. 683.
8. T. A. Kletz, *Learning from Accidents,* 2nd edition, Butterworth-Heinemann, Oxford, UK, 1994, Chapter 6.
9. *Report of the Investigation into the Fire at Amoco Refinery, 30 August 1983,* Dyfed County Fire Brigade, UK.

10. *Hazardous Cargo Bulletin,* Sept. 1983, p. 32; and Dec. 1983, p. 32.

11. T. E. Maddison, *Loss Prevention Bulletin,* No. 076, Aug. 1987, p. 31.

12. D. Nevill and G. C. White, "Research into the Structural Integrity of LNG Tanks," *New Directions in Process Safety,* Symposium Series No. 124, Institution of Chemical Engineers, 1991, p. 425 (discussion).

13. *Loss Prevention Bulletin,* No. 106, Aug. 1992, p. 5.

14. L. Streinbrecher, *Loss Prevention Bulletin,* No. 088, Aug. 1989, p. 25.

15. *Report of the Investigation into the Collapse of Tank 1338,* Commonwealth of Pennsylvania Department of Environmental Resources, Harrisburg, Pa., June 1988.

16. R. E. Sanders, *Management of Change in Chemical Plants—Learning from Case Histories,* Butterworth-Heinemann, Oxford, UK, 1993, p. 51.

17. F. E. Self and J. D. Hill, "Safety Considerations When Treating VOC Streams with Thermal Oxidizers," *Proceedings of the Thirty-first Annual Loss Prevention Symposium,* AIChE, New York, 1997.

18. *Loss Prevention Bulletin,* No. 131, Oct. 1996, p. 8.

19. N. Maddison, "Explosion Hazards in Large Scale Purification by Metal Dust," *Hazards XII—European Advances in Process Safety,* Symposium Series No. 134, Institution of Chemical Engineers, Rugby, UK, 1994.

20. R. S. Rowbottom, *Pulp and Paper Canada,* Vol. 90, No. 4, 1989, p. T138.

21. A. Trevitt, *The Chemical Engineer,* No. 27, Oct. 10, 1996, p. 27.

Chapter 6

Stacks

Stacks, like storage tanks, have been the sites of numerous explosions. They have also been known to choke.

6.1 STACK EXPLOSIONS

(a) Figure 6-1 shows the results of an explosion in a large flarestack. The stack was supposed to be purged with inert gas. However, the flow was not measured and had been cut back almost to zero to save nitrogen. Air leaked in through the large bolted joint between unmachined surfaces. The flare had not been lit for some time. Shortly after it was relit, the explosion occurred—the next time some gas was put to stack. The mixture of gas and air moved up the stack until it was ignited by the pilot flame.

To prevent similar incidents from happening again:

1. Stacks should be welded. They should not contain bolted joints between unmachined surfaces.
2. There should be a continuous flow of gas up every stack to prevent air diffusing down and to sweep away small leaks of air into the stack. The continuous flow of gas does not have to be nitrogen—a waste-gas stream is effective. But if gas is not being flared continuously, it is usual to keep nitrogen flowing at a linear velocity of 0.03–0.06 m/s. The flow of gas should be measured. A higher rate is required if hydrogen or hot condensable gases are being flared. If possible, hydrogen should be discharged through a separate vent stack and not mixed with other gases in a flarestack.

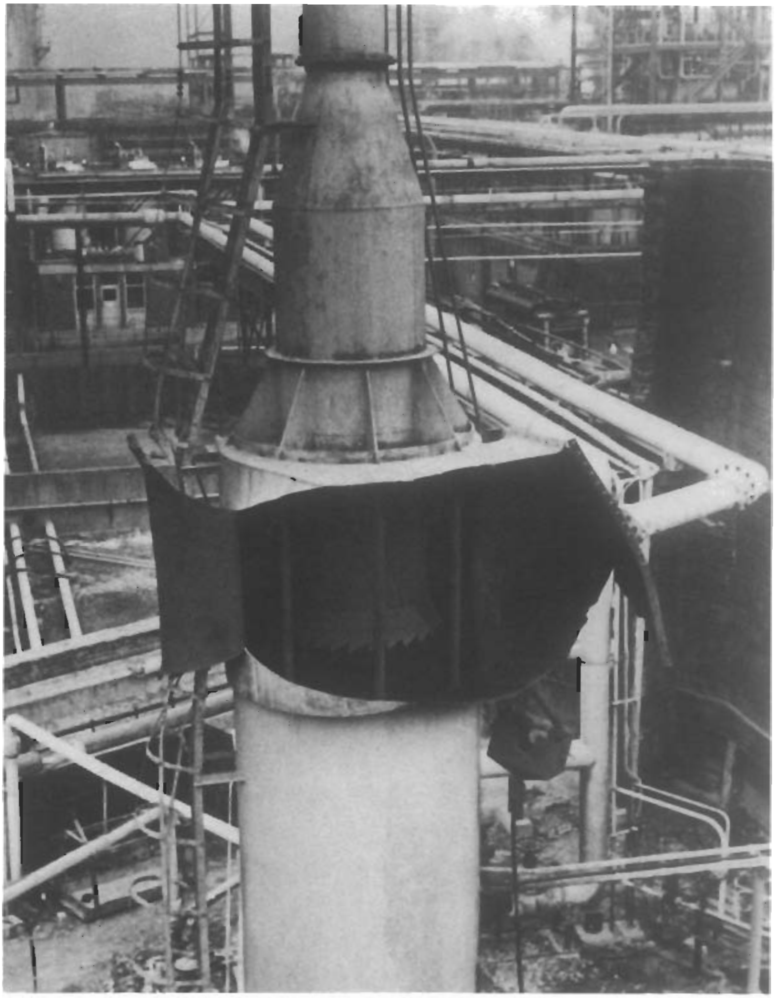


Figure 6-1. Base of flarestack.

3. The atmosphere inside every stack should be monitored regularly, say daily, for oxygen content. Large stacks should be fitted with oxygen analyzers that alarm at 5% (2% if hydrogen is present). Small stacks should be checked with a portable analyzer.

These recommendations apply to vent stacks as well as flarestacks.

(b) Despite the publicity given to the incident just described, another stack explosion occurred nine months later in the same plant.

To prevent leaks of carbon monoxide and hydrogen from the glands of a number of compressors getting into the atmosphere of the compressor house, they were sucked away by a fan and discharged through a small vent stack. Air leaked into the duct because there was a poor seal between the duct and the compressor. The mixture of air and gas was ignited by lightning.

The explosion would not have occurred if the recommendations made after the first explosion had been followed—if there had been a flow of inert gas into the vent collection system and if the atmosphere inside had been tested regularly for oxygen.

Why were they not followed? Perhaps because it was not obvious that recommendations made after an explosion on a large flarestack applied to a small vent stack.

(c) Vent stacks have been ignited by lightning or in other ways on many occasions. On several occasions, a group of ten or more stacks have been ignited simultaneously. This is not dangerous provided that:

1. The gas mixture in the stack is not flammable so that the flame cannot travel down the stack.
2. The flame does not impinge on overhead equipment. (Remember that in a wind, it may bend at an angle of 45°.)
3. The flame can be extinguished by isolating the supply of gas or by injecting steam or an increased quantity of nitrogen. (The gas passing up the stack will have to contain more than 90% nitrogen to prevent it from forming a flammable mixture with air.)

(d) A flare stack and the associated blowdown lines were prepared for maintenance by steaming for 16 hours. The next job was to isolate the system from the plant by turning a figure-8 plate in the 35-in. (0.9-m) blowdown line. As it was difficult to turn the figure-8 plate while steam escaped from the joint, the steam purge was replaced by a nitrogen purge two hours beforehand.

When the plate had been removed for turning, leaving a gap about 2 in. (50 mm) across, there was an explosion. A man was blown off the platform and killed.

The steam flow was 0.55 ton/hr, but the nitrogen flow was only 0.4 ton/hr, the most that could be made available. As the system cooled, air was drawn in. Some liquid hydrocarbon had been left in a blowdown vessel, and the air and hydrocarbon vapor formed a flammable mixture. According to the report, this moved up the stack and was ignited by the pilot burner, which was still lit. It is possible, however, that it was ignited by the maintenance operations.

As the steam was hot and the nitrogen was cold, much more nitrogen than steam was needed to prevent air from being drawn into the stack. After the explosion, calculations showed that 1.6 tons/hr were necessary, four times as much as the amount supplied. After the explosion, the company decided to use only nitrogen in the future, not steam [5].

Should the staff have foreseen that steam in the system would cool and that the nitrogen flow would be too small to replace it? Probably the method used seemed so simple and obvious that no one stopped to ask if there were any hazards.

(e) Three explosions occurred in a flarestack fitted, near the tip, with a water seal, which was intended to act as a flame arrestor and prevent flames from passing down the stack. The problems started when, as a result of incorrect valve settings, hot air was added to the stack that was burning methane. The methane/air mixture was in the explosive range, and as the gas was hot (300°C), the flashback speed from the flare (12 m/s) was above the linear speed of the gas (10 m/s in the tip, 5 m/s in the stack). An explosion occurred, which probably damaged the water seal, though no one realized this at the time. Steam was automatically injected into the stack, and the flow of methane was tripped. This extinguished the flame. When flow was restarted, a second explosion occurred, and as the water seal was damaged, this one traveled right down the stack into the knock-out drum at the bottom. Flow was again restarted, and this time the explosion was louder. The operating team then decided to shut down the plant [6]. We should not restart a plant after an explosion (or other hazardous event) until we know why it occurred.

(f) Another explosion, reported in 1997, occurred, like that described in (a) above, because the nitrogen flow to a stack was too low. It was cut back by an inexperienced operator; there was no low-flow alarm or high-oxygen alarm [7]. The author shows commendable

frankness in describing the incident so that others may learn from it, but nowhere in the report (or editorial comment) is there any indication that the lessons learned were familiar ones, described in published reports decades before.

For other stack explosions see Section 7.13 c and Reference 1.

6.2 BLOCKED STACKS

(a) Section 2.5 a described how an 8-in.-diameter vent stack became blocked by ice because cold vapor (at –100°C) and steam were passed up the stack together. The cold gas met the condensate running down the walls and caused it to freeze. A liquefied gas tank was overpressured, and a small split resulted. The stack was designed to operate without steam. But the steam was then introduced to make sure that the cold gas dispersed and did not drift down to ground level.

(b) The vent stack was replaced by a 14-in.-diameter flarestack with a supply of steam to a ring around the top of the stack. A few years later this stack choked again, this time due to a deposit of refractory debris from the tip, cemented together by ice (as some condensate from the steam had found its way down the stack). Fortunately, in this case the high pressure in the tank was noticed before any damage occurred. There was no boot at the bottom of the stack to collect debris (Figure 6-2). A boot was fitted [2].

(c) On other occasions, blowdown lines or stacks have become blocked in cold weather because benzene or cyclohexane, both of which have freezing points of 5°C, were discharged through them. Steam tracing of the lines or stacks may be necessary.

(d) Blowdown lines should never be designed with a dip in them, or liquid may accumulate in the dip and exert a back pressure. This has caused vessels to be overpressured [3].

(e) A blowdown line that was not adequately supported sagged when exposed to fire and caused a vessel to be overpressured.

(f) Water seals have frozen in cold weather. They should not be used except in locales where freezing cannot occur.

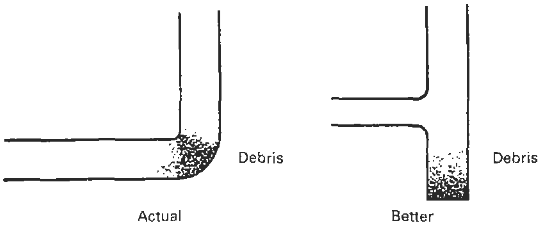


Figure 6-2. Flarestack after fall of debris.

Flare and vent systems should be simple. It is better to avoid water seals than install steam heating systems and low-temperature alarms, which might fail.

(g) Vent stacks are sometimes fitted with flame arrestors to prevent a flame on the end of the stack from traveling back down the stack. The arrestors are liable to choke unless regularly cleaned. They are also unnecessary, because unless the gas mixture in the stack is flammable, the flame cannot travel down the stack. If the gas mixture in the stack is flammable, then it may be ignited in some other way. Stacks should therefore be swept by a continuous flow of gas to prevent a flammable mixture from forming, as discussed in Section 6.1.

There are, however, two cases in which flame arrestors in vent stacks are justified:

1. If the gas being vented can decompose without the addition of air; an example is ethylene oxide. Whenever possible, such gases should be diluted with nitrogen. If this is not always possible, a flame arrestor may be used.
2. In the vent pipes of storage tanks containing a flammable mixture of vapor and air (Section 5.4.1). Such flame traps should be inspected regularly and cleaned if necessary. Section 5.3 a described how a tank was sucked in because the flame arrestors on all three vents had not been cleaned for two years.

A type of flame arrestor that can be easily removed for inspection without using tools is described in Reference 4.

(h) Molecular seals have been choked by carbon from incompletely burned gas, and water seals could be choked in the same way. For

this reason, many companies prefer not to use them. If they are partly choked, burning liquid or particles of hot carbon may be expelled when flaring rates are high [9] (see Section 5.5.2 d).

(i) The relief valve on a liquid hydrogen tank discharged to atmosphere through a short stack. The escaping hydrogen caught fire. The fire service poured water down the stack; the water froze, and the tank was overpressured and split. The fire should have been extinguished by injecting nitrogen up the stack, as discussed in Section 6.1 c.

The common theme of many of these items is that blowdown lines and flare and vent stacks should be kept simple because they are part of the pressure relief system. Avoid flame arrestors, molecular seals, water seals, and U-bends. Avoid steam, which brings with it rust and scale and may freeze.

6.3 HEAT RADIATION

The maximum heat radiation that people are exposed to from a flarestack should not exceed 4.7 kW/m^2 (1,500 $Btu/ft^2/hr$), about three times the peak solar radiation in the tropics. Even this amount of radiation can be withstood without injury for only a minute or two. The maximum to which people may be exposed continuously is about 1.7 kW/m^2 (500 $Btu/ft^2/hr$). In the neighborhood of flarestacks (say, wherever the radiation could exceed 1.7 kW/m^2), the temperatures reached by cables, roofing materials, and plastic equipment should all be reviewed to make sure they cannot be damaged [8, 9].

REFERENCES

1. J. L. Kilby, *Chemical Engineering Progress,* June 1968, p. 419.
2. T. A. Kletz, *Chemical Engineering Progress,* Vol. 70, No. 4, Apr. 1974, p. 80.
3. T. J. Laney, in C. H. Vervalin (editor), *Fire Protection Manual for Hydrocarbon Processing Plants,* Vol. 1, 3rd edition, Gulf Publishing Co., Houston, Texas, 1985, p. 101.

4. T. A. Kletz, *Learning from Accidents,* 2nd edition, Butterworth-Heinemann, Oxford, UK, 1994, Section 7.6.
5. *Loss Prevention Bulletin,* No. 107, Oct. 1992, p. 23.
6. V. M. Desai, *Process Safety Progress,* Vol. 15, No. 3, Fall 1996, p. 166.
7. T. Fishwick, *Loss Prevention Bulletin,* No. 135, June 1997, p. 18.
8. F. P. Lees, *Loss Prevention in the Process Industries,* 2nd edition, Butterworth-Heinemann, Oxford, UK, 1996, Chapter 16.
9. D. Shore, *Journal of Loss Prevention in the Process Industries,* Vol. 9, No. 6, Nov. 1996, p. 363.

Chapter 7

Leaks

A small leak will sink a great ship.

—Thomas Fuller, 1732

Leaks of process materials are the process industries' biggest hazard. Most of the materials handled will not burn or explode unless mixed with air in certain proportions. To prevent fires and explosions, we must therefore keep the fuel in the plant and the air out of the plant. The latter is relatively easy because most plants operate at pressure. Nitrogen is widely used to keep air out of low-pressure equipment, such as storage tanks (Section 5.4), stacks (Section 6.1), centrifuges (Section 10.1), and equipment that is depressured for maintenance (Section 1.3).

The main problem in preventing fires and explosions is thus preventing the process material from leaking out of the plant, that is, maintaining plant integrity. Similarly, if toxic or corrosive materials are handled, they are hazardous only when they leak.

Many leaks have been discussed under other headings, including leaks that occurred during maintenance (Chapter 1), as the result of human error (Chapter 3), or as the result of overfilling storage tanks (Section 5.1). Other leaks have occurred as the result of pipe or vessel failures (Chapter 9), while leaks of liquefied flammable gas are discussed in Chapter 8 and leaks from pumps and relief valves in Chapter 10.

Here, we discuss some other sources of leaks and the isolation and control of the leaking material.

7.1 SOME COMMON SOURCES OF LEAKS

7.1.1 Small Cocks

Small cocks have often been knocked open or have vibrated open. They should never be used as the sole isolation valve (and preferably not at all) on lines carrying hazardous materials, particularly flammable or toxic liquids, at pressures above their atmospheric boiling points (for example, liquefied flammable gases or most heat transfer oils when hot). These liquids turn to vapor and spray when they leak and can spread long distances.

It is good practice to use other types of valves for the first isolation valve, as shown in Figure 7-1.

7.1.2 Drain Valves and Vents

Many leaks have occurred because workers left drain valves open while draining water from storage tanks or process equipment and then returned to find that oil was running out instead of water.

In one incident, a man was draining water, through a 2-in.-diameter line, from a small distillation column rundown tank containing benzene. He left the water running for a few minutes to attend to other jobs. Either there was less water than usual or he was away longer than expected. He returned to find benzene running out of the drain line. Before he could close it, the benzene was ignited by the furnace which heated the distillation column. The operator was badly burned and died from his injuries.

The furnace was too near the drain point (it was about 10 m away), and the slope of the ground allowed the benzene to spread toward the

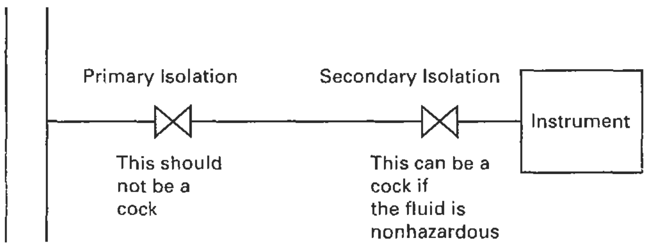


Figure 7-1. Small cocks should not be used as primary isolation valves.

furnace. Nevertheless, the fire would not have occurred if the drain valve had not been left unattended.

Spring-loaded ball valves should be used for drain valves. They have to be held open, and they close automatically if released. The size of drain valves should be kept as small as practicable. With liquefied flammable gases and other flashing liquids, ¾ in. should be the maximum allowed.

Drain valves that are used only occasionally to empty equipment for maintenance should be blanked when not in use. Regular surveys should be made to see that the blanks are in position. On one plant, a survey after a turnaround showed that 50 blanks were loose, each hanging on one bolt.

If water has to be drained regularly from liquefied flammable gases or other flashing liquids, and if a spring-loaded valve cannot be used, then a remotely operated emergency isolation valve (see Section 7.2.1) should be installed in the drain line.

When flammable materials are used, drain valves should not be located above hot pipework or equipment. A fire on an ethylene plant started when a mixture of water and naphtha was drained through a ¾-in. drain valve onto pipework at 315°C. It took a long time to replace damaged control and electric cables [21].

Drain valves should not be located above places where pools of water are liable to form, as leaks may then spread a long way (see Section 1.4.4).

While drain valves are installed to get rid of unwanted liquid, vent lines get rid of unwanted gas or vapor. They should be located so that the vapor is unlikely to ignite, so that damage is minimal if it does ignite, and so that people are not affected by the gas or vapor discharged. One fire destroyed a small plant. It started because the vent on a distillation column condenser discharged into the control room, possibly to prevent pollution of the surroundings, which had given rise to complaints about the smell [1] (see Section 2.11.3).

An electrician went up a ladder to repair a light fitting and was affected by fumes coming out of a vent about a meter away. The electrical hazards and the hazards of working from a ladder were considered, but no one thought about the hazards introduced by the vent—yet vents are designed to vent.

While contractors were working in a building, they inadvertently burned some insulation material. The ventilation system spread the fumes around the building. Two people were affected by them, and an expensive experiment taking place in a laboratory was ruined [15]. Before authorizing hot work in a building, consider the effects of any fumes that might be produced and, if necessary, switch off or isolate the ventilation system.

7.1.3 Open Containers

Buckets and other open-topped containers should never be used for collecting drips of flammable, toxic, or corrosive liquids or for carrying small quantities about the plant. Drips, reject samples, etc., should be collected in closed metal cans, and the caps should be fitted before the cans are moved.

One man was badly burned when he was carrying gasoline in a bucket and it caught fire. The source of ignition was never found. Another man was carrying phenol in a bucket when he slipped and fell. The phenol spilled onto his legs. One-half hour later he was dead. A third man was moving a small open-topped drum containing hot cleaning fluid. He slipped; liquid splashed onto him and scalded him.

A workman was draining hot tar from a portable kettle into a bucket when it caught fire. As he stepped back his glove stuck to the handle of the bucket, tipping it up and spilling the burning tar over the ground. The drain valve on the kettle was leaking, and this allowed the fire to spread. Two small liquefied-petroleum-gas containers (about 100 L), a trailer, and the kettle were destroyed. The end of one of the tanks was thrown 40 m [22].

Other incidents are described in Sections 12.2 c and 15.1.

These incidents may seem trivial compared with those described in other pages. But for the men concerned, they were their Flixborough.

Similarly, glass sample bottles should never be carried by hand. Workers have been injured when bottles they were carrying knocked against projections and broke. Bottles should be carried in baskets or other containers, such as those used for soft drinks. Bottles containing particularly hazardous chemicals, such as phenol, should be carried in closed containers.

Flammable liquids should, of course, never be used for cleaning floors or for cleaning up spillages of dirty oil. Use nonflammable solvents or water plus detergents.

7.1.4 Level and Sight Glasses

Failures of level glasses and sight glasses have caused many serious incidents. A leak of ethylene and an explosion that destroyed a plant may have been due to a level glass failure [2].

Level glasses and sight glasses (except magnetic types) should not be used on vessels containing flashing flammable or toxic liquids—that is, liquids under pressure above their normal boiling points. When level glasses are used, they should be fitted with ball check cocks, which prevent a massive leak if the glass breaks. Unfortunately, the balls have sometimes been removed by people who did not understand their purpose. The hand valves must be fully opened or the balls cannot operate (Figure 7-2).

A batch reactor was fitted with a rupture disc. A sight glass was fitted in a branch off the vent line so the disc could be inspected. When a runaway reaction occurred, the sudden rise in temperature and pressure broke the sight glass. Large amounts of flammable mist and vapor were discharged into the building, where they exploded, killing 11 people who had left the building but were standing outside [23]. The same reference describes other sight glass failures.

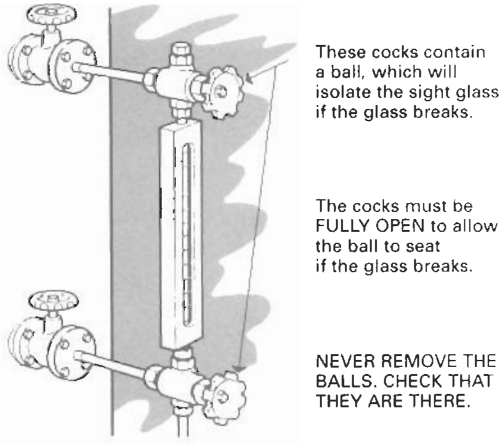


Figure 7-2. Ball check cocks.

7.1.5 Plugs

On many occasions screwed plugs have blown out of equipment.

(a) A ½-in. plug was fitted in a bellows (expansion joint) so that after pressure testing, in a horizontal position, water could be completely drained out. Soon after the bellows was installed, the plug blew out, followed by a jet of hot oil 30 m long.

Plugs installed to facilitate pressure testing should be welded in position. However, it is bad practice to seal weld over an ordinary screwed plug. If the thread corrodes, the full pressure is applied to the seal. A specially designed plug with a full-strength weld should be used.

(b) A 1-in. plug blew out of a pump body, followed by a stream of oil at 370°C and a gauge pressure of 250 psi (17 bar). The oil caught fire and caused extensive damage. The plug had been held by only one or two threads and had been in use for 18 years.

Following this incident, surveys at other plants brought to light many other screwed plugs, some held by only a few threads and some made from the wrong grade of steel. At one plant, which did not allow the use of screwed plugs, several 2-in. plugs were found, held by only one thread. They had been in use for ten years and were supplied as part of a compressor package.

A survey of all plugs is recommended.

(c) A similar incident is described in Section 9.1.6 (e). A screwed nipple and valve, installed for pressure testing, blew out of an oil line.

(d) The hinge-pin retaining plug on a standard swing check valve worked loose and blew out. Gas leaked out at a rate of 2 tons/hr until the plant could be shut down.

This incident emphasizes the point made in Section 7.2.1 (b). Check valves have a bad name among many plant operators, but no item of equipment can be expected to function correctly if it is never maintained.

(e) A valve was being overhauled in a workshop. A screwed plug was stuck in the outlet. To loosen the plug, the valve was heated with a welding torch. It shattered. The valve was in the closed position, and some water was trapped between the valve and the plug.

Valves should normally be opened before they are maintained.

7.1.6 Hoses

Hoses are a frequent source of leaks. The most common reasons have been:

1. The hose was made of the wrong material.
2. The hose was damaged.
3. The connections were not made correctly. In particular, screwed joints were secured by only a few threads, different threads were combined, or gaskets were missing.
4. The hose was fixed to the connector or to the plant by a screwed clip of the type used for automobile hoses (Jubilee clips). These are unsuitable for industrial use. Bolted clamps should be used.
5. The hose was disconnected before the pressure had been blown off, sometimes because there was no vent valve through which it could be blown off.
6. The hose was used for a service such as steam or nitrogen, and the service valve was closed before the process valve. As a result, process materials entered the hose.

These points are illustrated by the following incidents:

(a) It was decided to inject live steam at a gauge pressure of 100 psi (7 bar) into a distillation column to see if this improved its performance. An operator was standing in the position shown in Figure 7-3 and was about to close the inlet valve to the column when the hose burst. He was showered with hot, corrosive liquid. He was standing on an access platform. The leak prevented him from reaching the access ladder. He had to wait until someone fetched a portable ladder.

The investigation showed that:

1. The hose was made of reinforced rubber, the wrong material. A stainless steel hose should have been used.
2. The hose was damaged.
3. The steam valve at the other end of the hose was closed just before the column inlet valve, thus allowing process material to enter the hose. The operators knew this was not normal practice.

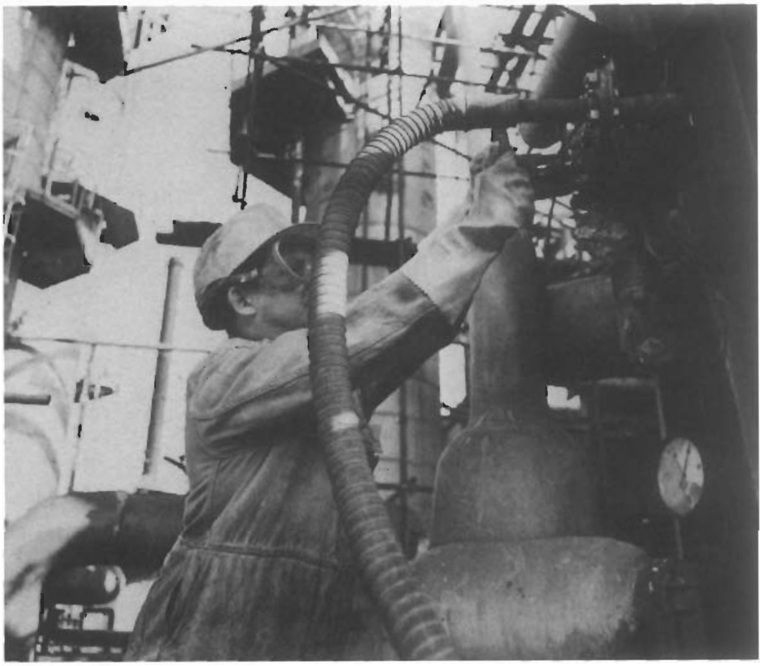


Figure 7-3. This hose burst, injuring the operator. It was the wrong type, was damaged, and was badly located.

But they closed the steam valve first because they knew the hose was damaged and wanted to avoid subjecting it to the full steam pressure.

The right type of hose should have been used, it should have been in good condition, and the process valve should have been closed first. In addition, a valve on a hose should not be in a position to which access is so poor. If no other valve was available, a steel pipe should have been fitted to the valve so that the end of the hose was in a safer place.

All hoses should be inspected and tested regularly and marked to show that they have been approved for use. A good practice is to change the color of the label every 6 or 12 months. This incident is a good illustration of the way both operators and managers become so used to the hazards of process materials that they fail to establish and maintain proper precautions. How often had the wrong

hose or a damaged hose been used before? Why had the foremen or the supervisors not noticed them?

(b) A tank truck containing 60% oleum arrived at a plant. The truck's hose was damaged, so the operators found a hose intended for use with 20% oleum. After 45 minutes it leaked, and there was a large spillage. The operators assumed the hose must have been damaged. They replaced it with a similar one, and after 15 minutes another spillage occurred.

This incident illustrates the mind-sets described in Section 3.3.5. Having assumed that a hose used for 20% oleum would be suitable for any sort of oleum, the operators stuck to their opinion even though the hose leaked. They thus had an "action replay." Sections 5.4.1 and 6.1 (c) describe other action replays.

Do your operators know which hoses are suitable for which materials? Mistakes are less likely if the number of different types used is kept to a minimum.

(c) A radioactive sludge was being pumped from a tank through a 1.5-in.-diameter hose into a moveable container. The pump stopped working, and a mechanic, asked to investigate, disconnected the hose using a quick-release coupling. Sludge was sprayed over three people standing up to 3 m away. There was no means of venting the pressure in the hose before uncoupling it. A choke in the hose prevented it from venting into the container, and it could not be vented through the positive displacement pump. The quick-release coupling could not be cracked open in the same way as a flange [24].

(d) This is a convenient place to describe a choke in a hose. To keep railway brake hoses clean before use, soft plastic "top hat" plugs were fitted into the ends. Each plug consisted of a closed cylinder, 7 mm long, which fitted into the end of a brake pipe, and a narrow lip, which was supposed to prevent it from going in too far (Figure 7-4 left). The plugs were colored red, the same color as the end of the brake pipe, so not surprisingly, a hose was fitted to a coach with the plug still in place. When the brakes were tested, the soft plug distorted and allowed compressed air to pass. Ultimately the plug moved into a position where it obstructed the pipe; a train failed to stop when required and overran by several miles. Fortunately the line was clear.

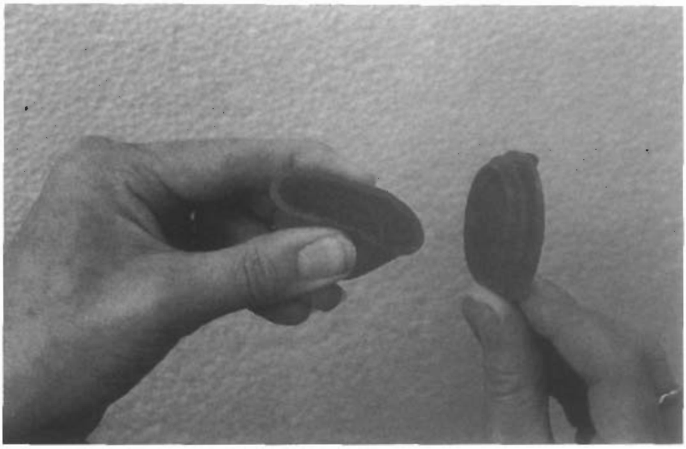


Figure 7-4. A soft plastic "top hat" plug (left) was fitted to the end of a railway carriage brake pipe to keep it clean. It was the same color as the end of the pipe and was not noticed and removed before the pipe was installed. The brakes failed, and the train overran. A more rigid plug with a larger lip (right) would have failed the brake test and would have been more visible. (*Photo courtesy of Roger Ford.*)

> A more rigid plug with a larger lip, as fitted to the other end of each pipe (Figure 7-4 right), would have caused the brake test to fail. The larger lip, and a different color, would have made the plug more visible. However, plastic bags tied over the ends would be a better way of keeping the hoses clean [25].

Other hose failures are described in Section 13.2.

7.1.7 Cooling Coils

The cooling coil in a storage tank developed a small leak. To prevent the liquid in the tank from leaking into the cooling water, the coil was isolated but kept up to pressure by closing and slip-plating the exit water valve but leaving the inlet valve open. The tank contained an aqueous solution of a toxic acid, so a small leak of water into the tank contents did not matter and was far preferable to a leak of the acid into the cooling water. Another coil provided all the cooling necessary.

Ten years later, there was a pressure surge on the cooling water lines when the cooling water pumps were changed over; this caused a sample

valve on the inlet water line to the coil to leak inside the building. The leaking water was contaminated with acid, which had been lying in the coil for ten years since the leak first occurred. There were no instructions for the changeover of the cooling water pumps, and on the occasion of the incident the valves were operated in an unusual order.

7.2 CONTROL OF LEAKS

7.2.1 Emergency Isolation Valves (EIVs)

Many fires have been prevented or quickly extinguished by remotely operated emergency isolation valves. We cannot install them in the lines leading to all equipment that *might* leak. However, we can install them in the lines leading to equipment that, experience shows, is particularly liable to leak (for example, very hot or cold pumps or drain lines, as described in Section 7.1.2) or in lines from which, if a leak did occur, a very large quantity of material, say 50 tons or more, would be spilled (for example, the bottoms pumps or reflux pumps on large distillation columns).

In all these cases, once the leak starts, particularly if it ignites, it is usually impossible to approach the normal hand-isolation valves to close them. Emergency isolation valves are discussed in detail in Reference 3, and the following incidents show how useful they can be. They can be operated electrically, pneumatically, or in some cases, hydraulically.

(a) A leak of light oil from a pump caught fire. The flames were 10 m high. From the control room, the operator closed a remotely operated valve in the pump suction line. The flames soon died down, and the fire burned itself out in 20 minutes. It would have been impossible to have closed a hand-operated valve in the same position. And if the emergency valve had not been provided, the fire would have burned for many hours. The emergency valve had been tested regularly. It could not be fully closed during testing but was closed part way.

 Backflow from the delivery side of the pump was prevented by a check (nonreturn) valve. In addition, a control valve and a hand valve well away from the fire were closed (Figure 7-5).

(b) The bearing on the feed pump to a furnace failed, causing a gland failure and a leak of hot oil. The oil caught fire, but an emergency isolation valve in the pump suction line was immediately closed, and the fire soon died out (Figure 7-6).

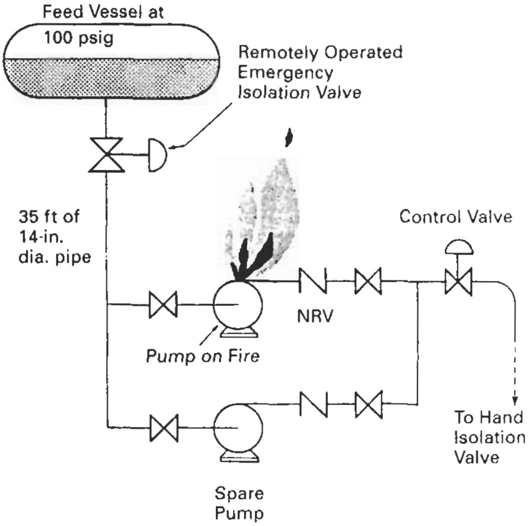


Figure 7-5. An emergency isolation valve stopped a fire.

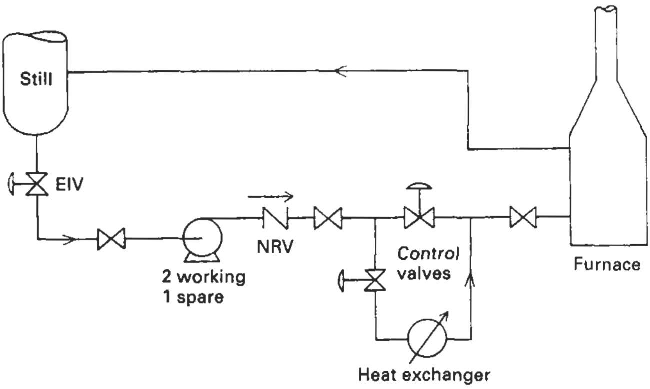


Figure 7-6. Another emergency isolation valve stopped a fire.

The control valve in the delivery line to the furnace was also closed. Unfortunately, this valve was bypassed by the line through the heat exchanger. In the heat of the moment, no one remembered to close the valve in the bypass line. In addition, the check (nonreturn) valve did not hold. The return flow of oil from the furnace was stopped by closing a hand valve next to the furnace, which was about 30 m from the fire. Afterward, another EIV was installed in the pump delivery line.

After the fire, the check valves on all three pumps were found to be out of order. On one the seat had become unscrewed. On another the fulcrum pin was badly worn. On the third the pin was worn right through, and the flap was loose. The valves had not been inspected since the plant was built.

Check valves have a bad name among many plant operators. However, this is because many of these valves are never inspected or tested. No equipment, especially that containing moving parts, can be expected to work correctly forever without inspection and repair. When check valves are relied on for emergency isolation, they should be scheduled for regular inspection.

Figure 7-7 shows a fluidic check valve that contains no moving parts. There is a low resistance to flow out of the tangential opening but high resistance to flow, 200 times higher, in the other direction. There is thus at times a small flow in the wrong direction, but if this can be tolerated the valves are very reliable and good at stopping pressure surges that might damage upstream equipment [26].

The EIV was not affected by the fire. But it was close to it, and the incident drew attention to the need to either place EIVs where they are unlikely to be affected by fire or to provide them with fire protection. Fire-resistant sacks and boxes are available [9, 10].

The impulse lines—electrical or pneumatic—leading to EIVs should also be fire-protected [11].

If control valves are used for emergency isolation, a special switch may be necessary, out on the plant, to close them in an emergency so that operators do not have to go to the control room to alter the set-points on the controllers.

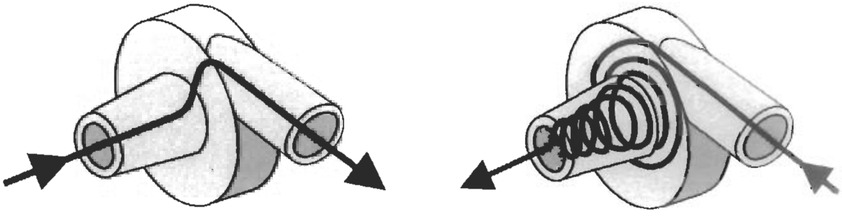


Figure 7-7. Fluidic check valve. (*Illustration courtesy of AEA Technology.*)

Note that the operation of an emergency isolation valve should automatically shut down any pump in the line and trip the fuel supply to any furnace.

(c) In contrast, on other occasions, EIVs failed to control fires because the installation was not up to standard. In one case, a fire burned for six hours because the button controlling the EIV was too close to the leaking pump for anyone to operate it safely [4]. It should have been at least 10 m away. In another case, an EIV failed to work because it had not been tested regularly. All EIVs should be tested regularly, say monthly. If they cannot be closed without upsetting production, they should be closed part way and tested fully at shutdowns.

(d) Emergency isolation valves are, of course, of no value if they are not used when required. Sometimes when there has been a leak of a hazardous material, the operators have been tempted to try to isolate the leak without shutting down the plant. In doing so they have taken unnecessary risks. For example, there was a bad leak of propylene on a pump inside a building. Four workers were badly injured. Afterward, a lot of money was spent on moving the pumps into the open air, surrounding them with a steam curtain [5] and fitting remotely operated isolation valves and blowdown valves. If another leak should occur, then it would be possible to stop the leak by closing the pump suction valve, opening the blowdown valve, and switching off the pump motor without any need for anyone to go near the pumps [16] (see Section 8.1.3).

Eight years went by before another bad leak occurred. When it did occur, the area around the pumps was filled with a visible cloud of propylene vapor 1 m deep. Instead of using the emergency equipment, which would have stopped the flow of propylene and shut down the plant, two very experienced foremen went into the compound, shut down the leaking pump, and started the spare up in its place. Fortunately the leak did not fire.

Afterward, when one of the foremen was back in his office, he realized the risk he had been taking. He complained that he should not be expected to take such risks. He had forgotten, in his eagerness to maintain production, that emergency equipment had been provided to avoid the need for such risk taking.

Other incidents that might have been controlled by EIVs are described in Sections 1.5.4 (e) and 16.1 (g).

EIVS should close quickly but not too quickly, or they may produce hammer pressures in the pipework, especially if the valves are located in long lines. An extra 30 seconds closing time is unlikely to be serious. Similarly, EIVs should not open too quickly. If there is a control valve in the pipework, it should also be closed to back up the EIV; afterward, it should be opened last, as it will open slowly [17].

The actuators fitted to EIVs should be somewhat more powerful than those recommended by manufacturers, especially if the liquid in the line is viscous. Some manufacturers do not allow for valve-packing friction forces [18]. EIVs, like all safety equipment, should be tested regularly (see Section 14.2.2).

7.2.2 Other Methods of Controlling Leaks

The following methods have been used successfully:

(a) Injecting water so that it leaks out instead of oil. This method can, of course, be used only when the water pressure is higher than the oil pressure.

(b) Reducing the plant pressure, thus reducing the size of the leak.

(c) Closing an isolation valve some distance away.

(d) Freezing a pipeline. This method requires time to organize the necessary equipment and can only be used with materials of relatively high freezing points, such as water or benzene.

(e) Injecting a sealing fluid into a leaking flange or valve gland using a proprietary process such as Furmaniting. Caution: accidents have occurred because correct procedures were not followed. Take care that bolts are not overstressed [12].

(f) Confining the spread of the leak by water spray [6, 8] or steam curtains [5]. The latter have to be permanently installed, but the former can be temporary or permanent.

(g) Controlling the evaporation from liquid pools by covering with foam. This method can be used for chlorine and ammonia spillages as well as hydrocarbon spillages if suitable foams are used.

(h) Adding a less volatile liquid to a spillage to reduce its volatility. When some liquefied petroleum gas (LPG) got into the drains,

some gas oil was poured down them to absorb the LPG and reduce the chance of an explosion.

7.2.3 How Not to Control a Leak

On many occasions employees have entered a cloud of flammable gas or vapor to isolate a leak. In the incident described in Section 7.2.1 (d), this was done to avoid shutting down the plant. More often, it has been done because there was no other way of stopping the leak. The persons concerned would have been badly burned if the leak had ignited while they were inside the cloud.

It would be going too far to say that no one should ever enter a cloud of flammable vapor to isolate a leak. There have been occasions when, by taking a risk for a minute, a man has isolated a leak that would otherwise have spread a long way and probably ignited, perhaps exploded. However, we should try to avoid putting people in such situations by providing remotely operated emergency isolation valves to isolate likely sources of leak.

It may be possible to isolate a leak by hand by forcing back the vapor with water spray and protecting the man who closes the valve in the same way. The National Fire Protection Association can provide a set of slides or a film showing how this is done.

It is possible to measure the extent of a leak of flammable gas or vapor with a combustible gas detector. If the leak is small, a person may be allowed (but not expected) to put his hands, suitably protected, inside the flammable cloud. But only in the most exceptional circumstances should a person be allowed to put more of his body into the cloud.

7.3 LEAKS ONTO WATER, WET GROUND, OR INSULATION

7.3.1 Leaks Onto Water or Wet Ground

Section 1.4.4 describes two leaks onto pools of water that spread much farther than anyone expected. One was ignited by a welder 20 m away, and the other spillage, onto a canal, caught fire 1 km away.

In other cases, spillages of oil have soaked into the ground and have then come to the surface after heavy rain. A spillage of gasoline in Essex, England, in 1966, came back to the surface two years later. The vapor accumulated on the ground floor of a house, ignited, and blew a hole in

the stairs, injuring two people. A trench 7 m deep was dug to recover the rest of the gasoline [7].

In other cases, spillages of oil have leaked into sewers and from there into houses.

If a substantial quantity of oil is spilled into the ground, attempts should be made to recover it by digging a well or trench.

7.3.2 Leaks Onto Insulation

When organic compounds come into contact with many hot insulation materials, they can degrade, and the auto-ignition temperature can fall by 100°–200°C. Many fires have started in this way (see Section 12.4.4). Most of them have been small, but some have been serious. For example, on a plant in Belgium in 1989, ethylene oxide (EO) leaked through a hairline crack in a weld on a distillation column and contaminated the rock wool insulation on a level indicator. The EO then reacted with moisture to form nonvolatile polyethylene glycols. The metal covering of the insulation was removed so the level indicator could be repaired. Air leaked in, and later the same day the polyethylene glycols ignited. This heated the wall of the piping system, in which there was no flow. The heat caused the EO to decompose explosively—a well-known reaction—and the decomposition traveled into the distillation column, which exploded. Figure 7-8 shows the result.

The source of ignition of the polyethylene glycol was probably auto-ignition of the degraded material. The report recommends the use of non-absorbent insulation for equipment containing heat-sensitive materials such as EO [19, 20].

In another incident, a long-chain alcohol leaked into the insulation of a pipeline. When the covering over the insulation was opened, allowing air to enter, the temperature (60°C) was sufficient for ignition [19].

7.4 DETECTION OF LEAKS

On many occasions combustible gas detectors have detected a leak soon after it started, and action to control it has been taken promptly. Installation of these detectors is strongly recommended whenever liquefied flammable gases or other flashing liquids are handled or when experience shows there is a significant chance of a leak [3]. Detectors are also

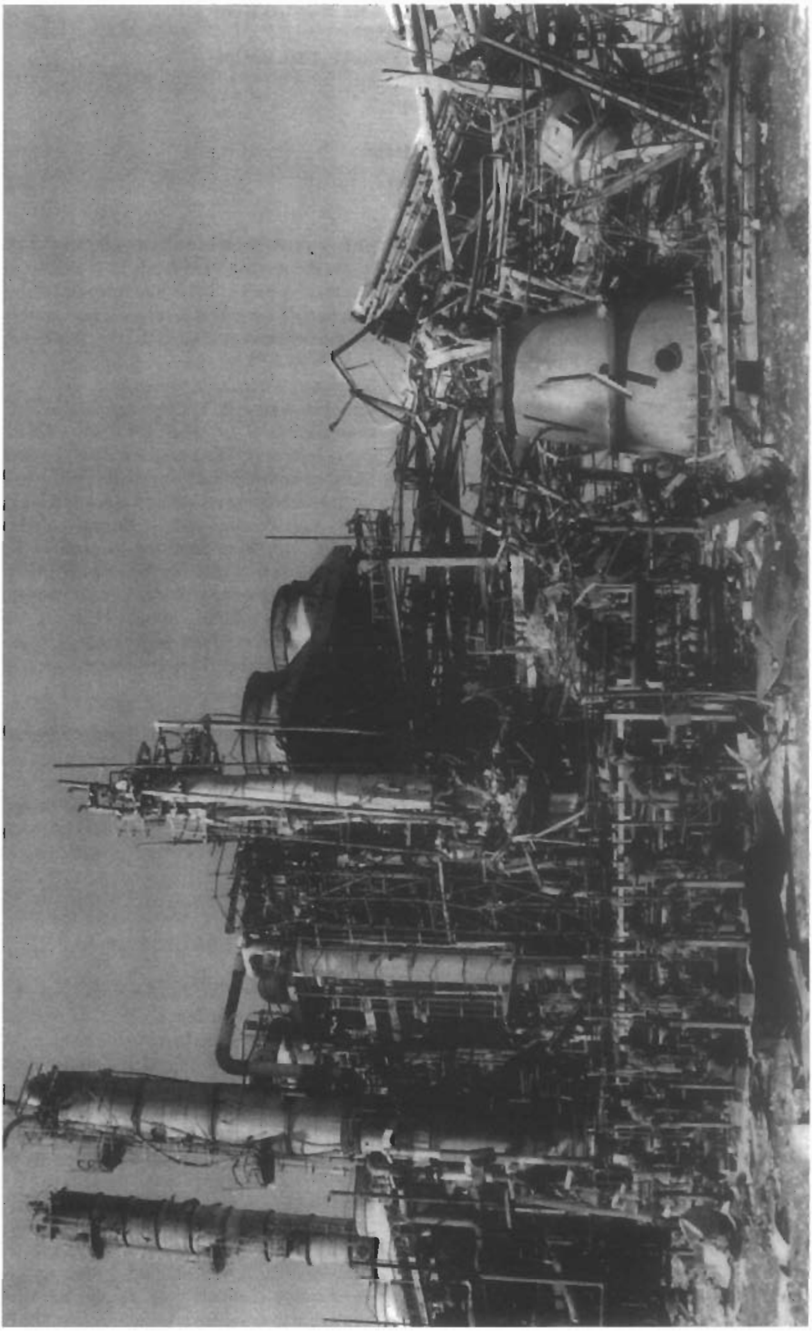


Figure 7-8. The ethylene oxide plant after the fire and explosion. (*Photo courtesy of BP Chemicals Limited.*)

available for common toxic gases. However, these detectors do not do away with the need for regular patrols of the plant by operators. Several plants that have invested heavily in gas detectors report that, nevertheless, half the leaks that have occurred have been detected by people.

On one plant, liquid leaks drained into a sump that was fitted with a level detector. When a leak actually occurred, it dripped onto a hot pipe and evaporated and was not detected for many hours (see Section 20.2.4).

A similar incident occurred on another plant. The liquid in the plant was cold, so a low-temperature alarm was installed in the sump. It was tested with cold water and worked well. When a leak occurred, the leaking liquid, which was acidic, reacted with the steelwork on its way to the sump and warmed up; the temperature element could not, of course, tell the difference between warm air and warm liquid and failed to detect the leak.

Whenever possible we should measure directly what we need to know and not some other property from which it can be deduced (see Section 14.6).

Electric cables that detect liquid leaks are available. They can be run through areas where leaks are possible, and they indicate the presence and location of a leak.

Large leaks can be detected by comparing flow rates in different parts of a plant. This can be done automatically on plants that are computer-controlled.

7.5 FUGITIVE EMISSIONS

There is increasing interest in fugitive emissions, small continuous leaks from flanges, valve and pump glands, relief valves, etc., which produce small but ever-present concentrations of chemicals in the workplace environment and some of which may produce long-term toxic effects. Reference 13 summarizes published data on the leak rates from various items of equipment and ways of reducing them. According to Reference 14, more than half the total emission from a refinery comes from valve glands. Actual figures are:

Source	Percent of Total Emission
Flanges	8
Valves	57
Compressors	3
Pumps	12
Relief valves	1
Separators	4
Cooling towers	7
Drains	8

REFERENCES

1. Health and Safety Executive, *The Explosion and Fire at Chemstar Ltd., 6 September 1981,* Her Majesty's Stationery Office, London, 1982.
2. C. T. Adcock and J. D. Weldon, *Chemical Engineering Progress,* Vol. 63, No. 8, Aug. 1967, p. 54.
3. T. A. Kletz, *Chemical Engineering Progress,* Vol. 71, No. 9, Sept. 1975, p. 63.
4. T. A. Kletz, *Hydrocarbon Processing,* Vol. 58, No. 1, Jan. 1979, p. 243.
5. H. G. Simpson, *Power and Works Engineering,* May 8, 1974, p. 8.
6. J. McQuaid and R. D. Fitzpatrick, *J. of Hazardous Materials,* Vol. 5, 1983, p. 121; and J. McQuaid, *J. of Hazardous Materials,* Vol. 5, 1983, p. 135.
7. *Petroleum Times,* Apr. 11, 1969.
8. K. Moodie, *Plant/Operations Progress,* Vol. 4, No. 4, Oct. 1985, p. 234.
9. M. Symalla, *Hydrocarbon Processing,* Vol. 63, No. 7, July 1984, p. 83.
10. A. E. Choquette, *Hydrocarbon Processing,* Vol. 63, No. 7, July 1984, p. 85.
11. G. K. Castle, *Hydrocarbon Processing,* Vol. 63, No. 3, Mar. 1984, p. 113.
12. H. J. Maushagen, *Loss Prevention Bulletin,* No. 055, Feb. 1984, p. 1.

13. British Occupational Hygiene Society, *Fugitive Emissions of Vapours from Process Equipment,* Report in *Science Reviews,* Northwood, UK, 1984.
14. C. R. Freeberg and C. W. Arni, *Chemical Engineering Progress,* Vol. 78, No. 6, June 1982, p. 35.
15. *Coordinating Construction/Maintenance Plans with Facility Manager May Deter Unexpected Problems and Accidents,* Safety Note DOE/EH-0127, U.S. Dept. of Energy, Washington, D.C., Apr. 1990.
16. T. A. Kletz, *Lessons From Disaster: How Organizations Have No Memory and Accidents Recur,* co-published by Institution of Chemical Engineers, Rugby, UK, and Gulf Publishing Co., Houston, Texas, 1993, Sections 2.2 and 8.10.
17. B. T. Matusz and D. L. Sadler, "A Comprehensive Program for Preventing Cyclohexane Oxidation Process Piping Failures," Paper presented at AIChE Loss Prevention Symposium, Houston, Texas, Mar./Apr. 1993.
18. *Undersized Valve Actuators,* Safety Note DOE/EH-0113, U.S. Dept. of Energy, Washington, D.C., Oct. 1989.
19. *Loss Prevention Bulletin,* No. 100, Aug. 1991, p. 1.
20. L. Britton, *Plant/Operations Progress,* Vol. 9, No. 2, Apr. 1990, p. 75; and Vol. 10, No. 1, Jan. 1991, p. 27.
21. *Loss Prevention Bulletin,* No. 131, Oct. 1996, p. 13.
22. *Occupational Health and Safety Observer,* Vol. 3, No. 12, U.S. Dept. of Energy, Washington, D.C., Dec. 1994, p. 4.
23. *Loss Prevention Bulletin,* No. 134, Apr. 1997, pp. 3, 5, and 6.
24. *Operating Experience Weekly Summary,* No. 96-45, Office of Nuclear and Facility Safety, U.S. Dept. of Energy, Washington, D.C., 1996, p. 10.
25. R. Ford, *Modern Railways,* Vol. 53, No. 579, Dec. 1996, p. 752.
26. Literature available from AEA Technology, Huntersville, N.C., and Warrington, UK.

Chapter 8

Liquefied Flammable Gases

This chapter describes a number of incidents involving liquefied flammable gases (LFG) that could have occurred only with these materials (or other flashing flammable liquids).

The property of LFG that makes it so hazardous is that it is usually stored and handled under pressure at temperatures above normal boiling points. Any leak thus flashes, much of it turning to vapor and spray. This can spread for hundreds of meters before it reaches a source of ignition.

The amount of vapor and spray produced can far exceed the theoretical amount of vapor produced, estimated by heat balance [1]. The vapor carries some of the liquid with it as spray. It may evaporate on contact with the air. In any case, it is just as likely to burn or explode.

Any flammable liquid under pressure above its normal boiling point will behave like LFG. Liquefied flammable gases are merely the most common example of a flashing liquid. Most unconfined vapor cloud explosions, including the one at Flixborough (Section 2.4), have been due to leaks of such flashing liquids [2].

The term *liquefied petroleum gas* (LPG) is often used to describe those liquefied flammable gases that are derived from petroleum. The term *LFG* is preferred when the discussion applies to all liquefied flammable gases. It includes materials such as ethylene oxide, vinyl chloride, and methylamines, which behave similarly so far as their flashing and flammable properties are concerned.

LFGs stored at atmospheric pressure and low temperature behave rather differently from those stored under pressure at atmospheric tem-

perature. Incidents involving these materials are described in Sections 2.5, 5.2.2 d, 5.6.2, and 8.1.5.

8.1 MAJOR LEAKS

8.1.1. Feyzin

The bursting of a large pressure vessel at Feyzin, France, in 1966 was at the time one of the worst incidents involving LFG that had ever occurred but has since been overshadowed by the events at Mexico City (see Section 8.1.4). It caused many companies to revise their standards for the storage and handling of these materials. Because no detailed account has been published, it is described here. The information is based on References 3 through 6 and on a discussion with someone who visited the site soon after the fire.

An operator had to drain water from a 1,200-m^3 spherical storage vessel nearly full of propane (Figure 8-1). He opened valves A and B. When traces of oil showed that the draining was nearly complete, he shut A and then cracked it to complete the draining. No flow came. He opened A fully. The choke—presumably hydrate, a compound of water and a light hydrocarbon with a melting point above 0°C—cleared suddenly, and the operator and two other men were splashed with liquid. The handle came off valve A, and they could not get it back on. Valve B was frozen and could not be moved. Access was poor because the drain valves were immediately below the tank, which was only 1.4 m above the ground.

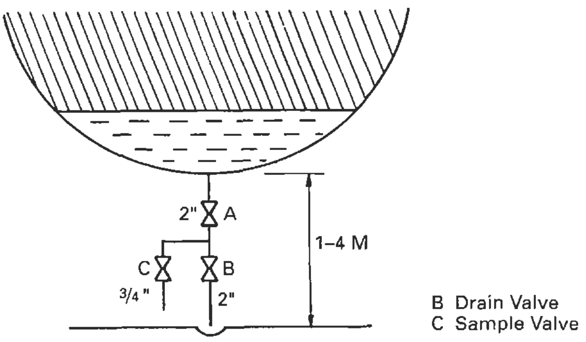


Figure 8-1. Drain valves underneath propane tank at Feyzin.

A visible cloud of vapor, 1 m deep, spread for 150 m and was ignited by a car that had stopped on a nearby road 25 minutes after the leak started. The road had been closed by the police, but the driver approached from a side road. The fire flashed back to the sphere, which was surrounded by flames. There was no explosion. The sphere was fitted with water sprays. But the system was designed to deliver only half the quantity of water normally recommended (0.2 U.S. gal/ft^2 min. or 8 L/m^2 min.), and the supply was inadequate. When the fire brigade started to use its hoses, the supply to the spheres ran dry. The firemen seemed to have used most of the available water for cooling neighboring spheres to stop the fire from spreading, in the belief that the relief valve would protect the vessel on fire.

The ground under the sphere was level so that any propane that did not evaporate or burn immediately collected under the sphere and burned later.

Ninety minutes after the fire started, the sphere burst. Ten out of 12 firemen within 50 m were killed. Men 140 m away were badly burned by a wave of propane that came over the compound wall. Altogether, 15-18 men were killed (reports differ), and about 80 were injured. The area was abandoned. Flying debris broke the legs of an adjacent sphere, which fell over. Its relief valve discharged liquid, which added to the fire, and 45 minutes later this sphere burst. Altogether, five spheres and two other pressure vessels burst, and three were damaged. The fire spread to gasoline and fuel oil tanks.

At first it was thought that the spheres burst because their relief valves were too small. But later it was realized that the metal in the upper portions of the spheres was softened by the heat and lost its strength. Below the liquid level, the boiling liquid kept the metal cool. Incidents such as this one in which a vessel bursts because the metal gets too hot are known as Boiling Liquid Expanding Vapor Explosions or BLEVEs.

To prevent such incidents from occurring, many companies—after Feyzin—adopted recommendations similar to the following:

Recommendations to prevent a fire from starting [7]

- Restrict the size of the second drain valve to ¾ in., and place it at least 1 m from the first valve. The drain line should be robust and firmly supported. Its end should be located outside the shadow of the tank.
- Fit a remotely controlled emergency isolation valve (see Section 7.2.1) in the drain line.

- New installations should be provided with only one connection below the liquid level, fully welded up to a first remotely operated fire-safe isolation valve located clear of the tank area.
- Install combustible gas detectors to provide early warning of a leak.

Recommendations to prevent a fire from escalating [7, 8]

- Insulate vessels with a fire-resistant insulation, such as vermiculite concrete. This is available as an immediate barrier to heat input. Unlike water spray, it does not have to be commissioned.

  In some countries, mounding is used instead of conventional insulation. The tank is completely covered with clean sand or other clean material. Portions of the covering must be removed from time to time so that the outside of the tank can be inspected.
- Provide water spray or deluge (unless the vessel is mounded). If insulation is provided, then water deluge at a rate of 0.06 U.S. gal/ft^2 min. (2.4 L/m^2 min.) is sufficient. If insulation is not provided, then water spray at a rate of 0.2 U.S. gal/ft^2 min. (8 L/m^2 min.) is necessary. (Deluge water is poured on the top of a vessel; spray is directed at the entire surface.)
- Slope the ground so that any spillage runs off to a collection pit.
- Fit an emergency depressuring valve so that the pressure in the vessel can be reduced to one fifth of design in ten minutes to reduce the strain on the metal [13]. The time can be increased to 30 minutes if the vessel is insulated and to one hour if, in addition, the ground is sloped.

Figure 8-2 summarizes these proposals.

8.1.2 Duque De Caxias

A similar incident to that at Feyzin occurred at this refinery in Brazil in 1972. According to press reports, the relief valve failed to open when the pressure in an LPG sphere rose. To try to reduce the pressure, the operators opened the drain valve. Little water came out, and the LPG that followed it caused the valve to freeze, and the flow could not be stopped. There was only one drain valve. The LPG ignited, the vessel BLEVEd, and 37 people were killed.

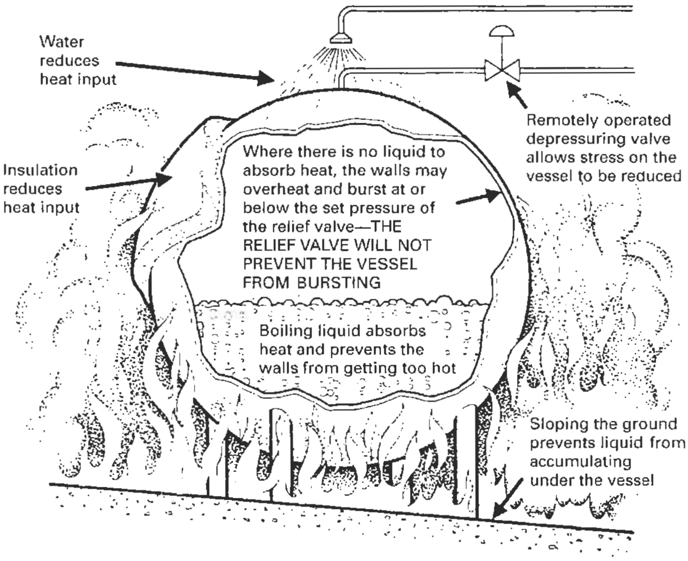


Figure 8-2. Methods of protecting a pressure vessel against fire.

If the operators did, in fact, try to reduce the pressure by draining water. they did not realize that the vapor pressure above a liquid is the same whatever the quantity present.

8.1.3 United Kingdom

This fire occurred some years ago because those concerned did not fully appreciate the difference in behavior between liquid hydrocarbons, such as naphtha or gasoline, and LFGs. The vapor from a spillage of gasoline will spread only a short distance—about the diameter of the pool. But the vapor from a spillage of LFG can spread for hundreds of meters.

Some equipment that had been designed and used for handling gasoline and similar liquids was adapted to handle propylene. A leak occurred from the gland of a high-pressure reciprocating pump operating at a gauge pressure of 3,625 psi (250 bar) due to the failure of the studs holding the gland in position. The pump was located in an unventilated building. But the vapor escaped through a large doorway opposite the pump and was ignited by a furnace 75 m away. Four men were badly burned.

The vapor from a spillage of gasoline in the same position would not have spread anywhere near the furnace.

After the fire, the pump (and others) was relocated in the open air, under a canopy, so that small leaks would be dispersed by natural ventilation. It was surrounded by a steam curtain to disperse larger leaks. This would not have been necessary if the pump could have been located more than 150 m from sources of ignition. Gas detectors were installed to give early warning of any leaks. Emergency isolation valves (Section 7.2.1) were provided so that the pumps could be isolated safely from a distance [9]. What happened when another leak occurred is described in Section 7.2.1 (d).

Note that a common factor in incidents 8.1.1 through 8.1.3 was a failure by those concerned to understand the properties of the materials and equipment.

8.1.4 Mexico City

The fire and explosion at a processing plant and distribution center for liquefied petroleum gas (LPG—actually 80% butane, 20% propane) in San Juanico, a suburb of Mexico City, in November 1984, was one of the worst incidents that has ever occurred in the oil and chemical industries, exceeded only by Bhopal. According to official figures, 542 people were killed, 4,248 injured, and about 10,000 made homeless; but unofficial estimates are higher. The disaster started when an 8-in. LPG pipeline ruptured. The reason for the failure is not known, but according to one report [14] a tank was overfilled and the inlet line overpressured. It is not clear why the relief valve did not lift. The gas cloud covered an area of 200 m by 150 m before it was ignited, probably by a ground-level flare, about 5–10 minutes after the leak started. The gas cloud burned and disappeared, but a flame was left burning near the broken pipe, and this flame heated an LPG sphere, which BLEVEd, causing further damage and further BLEVEs. Altogether, four spheres and 15 cylindrical tanks BLEVEd during the next 1½ hours, and some of the tanks landed up to 1,200 m from the plant [15].

Most of those killed and injured were members of the public who were living in a shanty town near the plant. When the plant was built, the nearest houses were 360 m away, but homes had been allowed to encroach on the intervening ground until the nearest houses were only 130 m from the plant.

Although much of the plant was only a few years old (some parts were 20 years old), most of the recommendations made in Section 8.1.1 and taken from a report published in 1970 [7] do not seem to have been followed in the design. For example, there were no gas detectors, the water deluge system was inadequate (or failed to operate), there was little or no fire insulation (even the legs of the spheres were not insulated), bunds around the vessels allowed LPG to accumulate where it could do most harm, and there were many connections to vessels below the liquid level [16]. In addition, the plant seems to have been congested and was much too near concentrations of people. A typical recommended distance for a large LPG processing area is 600 m [17], not 360 m, the original distance, or 130 m, the distance at the time. At Bhopal also (see Section 21.1), uncontrolled spread of a shanty town was responsible for the large number of casualties.

8.1.5 Qatar

The incidents described so far involved LFG stored under pressure at atmospheric temperature. LFG can also be stored at a low temperature and atmospheric pressure, and this method is often preferred for large storages because, due to the low pressure, the leak rate through a hole of a given size is smaller, and due to the low temperature, the evaporation rate is smaller. However, when deciding on the method of storage to be used, the probability of a leak from the installation as a whole, including the refrigeration and vaporization plants, should be considered. There will be no gain if we reduce the chance of a leak from the storage tanks but introduce extra equipment that is more likely to leak.

In 1977, the technical press reported that a major leak from a 20,000-m^3 liquefied propane tank in Qatar had ignited and that the resulting fire and explosion had killed seven people and caused extensive damage to the rest of the plant [18]. There had also been a leak the year before, but it had not ignited, and the tank had been repaired. The propane was stored at −42°C and atmospheric pressure. No detailed report on the incident was issued, for legal reasons, but a member of the company concerned published several papers [19–21], which gave new recommendations for the construction of tanks for refrigerated LFG, and it is thus possible to read between the lines and surmise what probably happened.

The new recommendations said that refrigerated LFG tanks should be made from materials such as 9% nickel steel, which will not propagate a

crack if one should start. Previously, the policy of many companies was to prevent cracks rather than rely on the crack-arresting properties of the tank material. It thus seems that at Qatar a crack started, despite the precautions taken to prevent such an occurrence, and then propagated rapidly. The reason for the initial crack is not known. It may have been connected with the repairs that were carried out following the crack the previous year. According to one report [22], this crack was due to weld attack by bacteria in the seawater used for pressure testing. However, the cause of the crack is of secondary importance compared with the fact that once it appeared it spread rapidly.

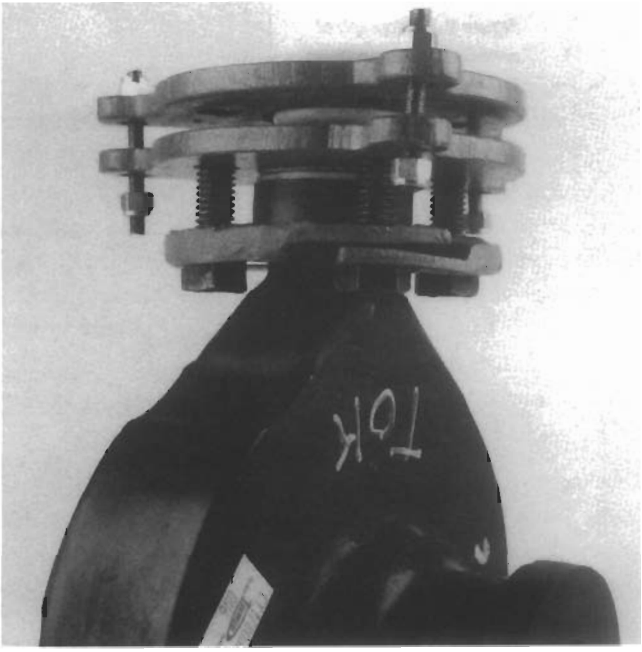
It is now widely recognized that we cannot prevent fires and explosions by eliminating sources of ignition. We do what we can, but they are still liable to turn up. So we try to prevent the formation of explosive mixtures. Similarly, it is now argued that we cannot eliminate all causes of cracks, and so we should make sure that any that do occur do not propagate.

At Qatar, the liquid came out with such force that it spilled over the dike wall. Conventional dike walls also have the disadvantage that a large area of liquid is exposed to the atmosphere if a leak occurs. For these reasons it is now usual to surround cryogenic storage tanks with a concrete wall, about 1 m from the tank and the full height of the tank. If the tank is not made from crack-resistant material, then the concrete wall should be designed to withstand the effects of a sudden release of liquid.

8.1.6 Ethyl Chloride Plant

In 1994 a leak of impure ethyl chloride (boiling point 12°C) caught fire, 1½ hours after it started, and damaged the plant so extensively that it had to be rebuilt. Fortunately, no one was killed or injured. The leak started at a flange assembly on the delivery of a pump (Figure 8-3), probably due to corrosion of the flanges but possibly due to failure of a plastic bellows. The official report [23] made the following points:

- The split flanges were badly corroded; their thickness was reduced, and the bolt holes were much enlarged. (Split flanges are not a good feature because they expose twice as much surface to the effects of corrosion.) There was no system for identifying critical items, the failure of which could have serious results, and registering them for regular inspection. Maintenance was on a breakdown basis, and there



(Photo courtesy of the UK Health and Safety Executive.)

Figure 8-3. Split flange assembly similar to one that leaked.

were no formal records that could be used to identify items needing regular inspection or replacement.

- The leak could have been stopped as soon as it was detected if an emergency isolation valve (Section 7.2.1) had been fitted in the pump suction line. On the rebuilt plant such valves were fitted on the pump suction lines, more combustible gas detectors and more extensive insulation were installed, plastic pump bodies were replaced by metal ones, and spillages were directed to collection pits. The plant was built in 1972, when these features were not common practice; many improvements had been made since then, but they did not go far enough. Most of those made after the fire could have been made beforehand.
- The source of ignition may have been a box containing electrical equipment. It had a badly fitted or incorrect type of plug, which could have allowed water to enter and to cause arcing.

- The fire was more serious than it would normally have been because the inventory in the plant, about 70 tons, was about twice the usual amount. Some of the overheads from a reactor were collected in a slops drum and recycled. The inventory in the drum was usually small. At about 9 a.m. on the day of the fire, the recycle pump failed. As a result, the level in the drum rose, and the level in the reactor fell. The operator noticed the fall in the reactor level (but not the rise in the drum level) and recycled product to maintain the level. At 8 p.m. the supervisor noticed that the high-level alarm on the slops drum was lit; he found that the recycle pump had failed, and he changed over to the spare; it leaked 25 minutes later. Section 3.3.1 describes another occasion when operators failed to notice unusual readings for 11 hours.
- The major hazard on the site as a whole was the storage and use of chlorine. So much attention was devoted to this that other hazards received less attention than they should have.
- The official report sums up the lessons of the fire by saying that it might have been prevented or its severity greatly reduced if a more detailed assessment of the inherent hazards and risks of the plant had been carried out by the company beforehand and if adequate records had been kept to build up a history on which an inspection and replacement program could have been based.

8.2 MINOR LEAKS

(a) After Feyzin (see Section 8.1.1) one company spent a lot of money improving the standard of its LFG storage facilities—in particular, the water-draining arrangements—so as to comply with the recommendations made in Section 8.1.1.

Less than a year later, a small leak from a passing drain valve on a pipeline caught fire. It was soon extinguished by closing the valve. But an investigation disclosed that:

1. There should have been two valves in series or a single valve and blank.
2. The valve was made of brass and was of a type stocked for use on domestic water systems. It was not the correct pressure rating for LFG.

3. The valve was screwed onto the pipeline, though the company's codes made it clear that only flanged or welded joints were allowed.
4. It was never discovered who installed this unauthorized substandard drain point. An attempt had been made to publicize the lessons of Feyzin, the company's standards, and the reasons for them. However, this did not prevent the installation of the drain point. Note that a number of people must have been involved. Besides the man who actually fitted it and his foreman, someone must have issued a work permit and accepted it back (when he should have inspected the job), and several persons must have used the drain point. Many must have passed by. If only one of them had recognized the substandard construction and drawn it to the attention of those responsible, the fire would not have occurred [10].

Like the plants in our gardens, our plants grow unwanted branches while our backs are turned.

(b) A propane sphere was filled with water to inert it during repair work. When the repairs were complete, the water was drained from the sphere, and propane vapor was admitted to the top to replace the water. The instruction stated that draining should stop when 5 m^3 of water was left in the vessel. But no one was present when this stage was reached. All the water drained out, followed by propane. Fortunately it did not ignite. The job had been left because the operators did not realize that the level indicator, which measured weight, would indicate a level of water almost twice the actual level. Other similar incidents are described in Section 5.1.2. If nitrogen is available, it should be used instead of water for inerting vessels. Or if water is used, it should be replaced by nitrogen when it is drained. Before filling any equipment with water, always check that it is strong enough to take the weight of the water [11].

8.3 OTHER LEAKS

Numerous leaks of LFG, mainly minor but occasionally more serious, have occurred from the following items of equipment:

Flanged joints

The size and frequency of leaks can be reduced by using spiral-wound gaskets in place of compressed asbestos fiber ones. Screwed joints should not be used.

Pump seals

The leak size can be reduced by using double mechanical seals or a mechanical seal and a throttle bush, the space between the two being vented to a safe place. Major leaks may still occur, however, due to collapse of the bearing or seal. LFG pumps should therefore be fitted with emergency isolation valves (see Section 7.2.1), particularly if the temperature is low or the inventory that can leak out is high.

Level glasses

These should not be used with flashing flammable liquids (see Section 7.1.4).

Sample points

These should not exceed ¼-in. diameter.

Small branches

These should be physically robust and well supported so they cannot be knocked off accidentally or vibrate until they fail by fatigue.

Equipment made from grades of steel unsuitable for use at low temperatures

Materials of construction should be chosen so the equipment will withstand the lowest temperature that can be reached during abnormal operation. In the past, materials have been used that will withstand normal operating temperatures but that may become brittle at lower temperatures reached during plant upsets or abnormal operation, for example, when the pressure in a vessel containing liquefied petroleum gas is reduced and the vessel is cooled by evaporation of the liquid (see Section 10.5.2). Some spectacular failures have resulted [12] (see Section 9.2.1 g).

Wholesale replacement of such materials in existing plants is impractical, and there is no universal solution. Some lines can be replaced in different grades of steel. Sometimes low temperature trips or alarms can be used. Sometimes the need to watch the temperature closely during start-up has to be impressed on operators.

Other leaks of LFG are described in Sections 1.1.6 (e), 1.5.4 (a), 5.2.2 (d), 9.1.6 (d) and (f), and 13.4.

REFERENCES

1. J. D. Reed, "Containment of Leaks from Vessels Containing Liquefied Gases with Particular Reference to Ammonia," *Proceedings of the First International Symposium on Loss Prevention and Safety Promotion in the Process Industries,* Elsevier, Amsterdam, 1977, p. 191.
2. J. A. Davenport, *Chemical Engineering Progress,* Vol. 73, No. 9, Sept. 1977, p. 54.
3. *The Engineer,* Mar. 25, 1966, p. 475.
4. *Paris Match,* No. 875, Jan. 15, 1966.
5. *Fire,* Special Supplement, Feb. 1966.
6. *Petroleum Times,* Jan. 21, 1966, p. 132.
7. Imperial Chemical Industries Ltd., *Liquefied Flammable Gases—Storage and Handling,* Royal Society for the Prevention of Accidents, Birmingham, UK, 1970.
8. T. A. Kletz, *Hydrocarbon Processing,* Vol. 56, No. 8, Aug. 1977, p. 98.
9. T. A. Kletz, *Lessons From Disaster: How Organizations Have No Memory and Accidents Recur,* co-published by Institution of Chemical Engineers, Rugby, UK, and Gulf Publishing Co., Houston, Texas, 1993, Section 2.2.
10. T. A. Kletz, *Chemical Engineering Progress,* Vol. 72, No. 11, Nov. 1976, p. 48.
11. *Petroleum Review,* Apr. 1982, p. 35.
12. A.L.M. van Eijnatten, *Chemical Engineering Progress,* Vol. 73, Sept. 1977.
13. R. S. Sonti, *Chemical Engineering,* Jan. 23, 1984, p. 66.

14. J. A. Davenport, "Hazards and Protection of Pressure Storage of Liquefied Petroleum Gases," *Proceedings of the Fifth International Symposium on Loss Prevention and Safety Promotion in the Process Industries,* Société de Chimie Industrielle, Paris, 1986, p. 22-1.
15. *BLEVE! The Tragedy of San Juanico,* Skandia International Insurance Corporation, Stockholm, Sweden, 1985.
16. *The Chemical Engineer,* No. 418, Oct. 1985, p. 16 (contains a series of articles on Mexico City).
17. T. A. Kletz, *Loss Prevention,* Vol. 13, 1980, p. 147.
18. *Middle East Econ. Digest,* Vol. 21, Apr. 15, 1977, and July 1, 1977.
19. N. J. Cupurus, "Cryogenic Storage Facilities for LNG and NGL," *Proceedings of the Tenth World Petroleum Congress,* Heyden, London, 1979, p. 119 (Panel Discussion 17, Paper 3).
20. N. J. Cupurus, "Developments in Cryogenic Storage Tanks," Paper presented at 6th International Conference on Liquefied Natural Gas, Kyoto, Japan, 1980.
21. N. J. Cupurus, "Storage of LNG and NGL," Paper presented at Seminar on LNG and NGL in Western Europe in the 1980s, Oslo, Norway, Apr. 2, 1981, Session II.
22. *One Hundred Largest Losses—A Thirty Year Review of Property Damage Losses in the Hydrocarbon-Chemical Industries,* 9th edition, M&M Protection Consultants, Chicago, 1986.
23. Health and Safety Executive, *The Chemical Release and Fire at the Associated Octel Company Limited,* HSE Books, Sudbury, UK, 1996.

Chapter 9

Pipe and Vessel Failures

It happens, like as not,
There's an explosion and good-bye the pot!
These vessels are so violent when they split
Our very walls can scarce stand up to it.

—Geoffrey Chaucer, "The Canon Yeoman's Tale," c. 1386

9.1 PIPE FAILURES

Davenport [1] has listed more than 60 major leaks of flammable materials, most of which resulted in serious fires or unconfined vapor cloud explosions. Table 9-1, derived from his data, classifies the leak by point of origin and shows that pipe failures accounted for half the failures—more than half if we exclude transport containers. It is therefore important to know why pipe failures occur. Following, a number of typical failures (or near failures) are discussed. These and other failures, summarized in References 2 and 3, show that by far the biggest single cause of pipe failures has been the failure of construction teams to follow instructions or to do well what was left to their discretion. The most effective way of reducing pipe failures is to:

1. Specify designs in detail.
2. Check construction closely to see that the design has been followed and that details not specified have been constructed according to good engineering practice.

Table 9-1
Origin of Leaks Causing Vapor Cloud Explosions

Origin of Leak	Number of Incidents	Notes
Transport container	10	Includes 1 zeppelin
Pipeline (incl. valve, flange, sight-glass, etc.)	34	Includes 1 sight-glass and 2 hoses
Pump	2	
Vessel	5	Includes 1 internal explosion, 1 slopover, and 1 failure due to overheating
Relief valve or vent	8	
Drain valve	4	
Error during maintenance	2	
Unknown	2	
Total	**67**	

Many publications about pipe failures attribute them to causes such as fatigue or inadequate flexibility. This is not very helpful. It is like saying a fall was caused by gravity. We need to know why fatigue occurred or why the flexibility was inadequate. To prevent further incidents, should we improve the design, construction, operations, maintenance, inspection, or what? The following incidents, and many others, suggest that improvement should be made to the design/construction interface. That is, we should focus on the detailing of the design and see that it has been followed and that good practice has been followed when details are not specified.

9.1.1 Dead-ends

Dead-ends have caused many pipe failures. Water, present in traces in many oil streams, collects in dead-ends and freezes, breaking the pipe. Or corrosive materials dissolve in the water and corrode the line.

For example, there was a dead-end branch, 12 in. in diameter and 3 m long, in a natural-gas pipeline operating at a gauge pressure of 550 psi (38 bar). Water and impurities collected in the dead-end, which corroded and failed. The escaping gas ignited at once, killing three men who were looking for a leak [4].

There are other sorts of dead-ends besides pipes that have been blanked. Rarely used valved branches are just as dangerous. The feed line to a furnace (Figure 9-1) was provided with a permanent steam connection for use during de-coking.

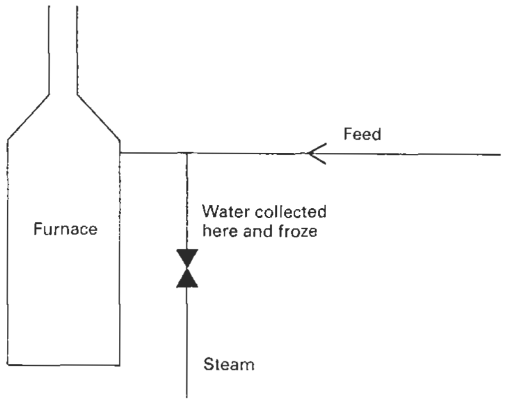


Figure 9-1. The steam connection to the furnace formed a dead-end.

The connection was on the bottom of the feed line, and the steam valve was not close to the feed line. Water collected above the steam valve, froze during cold weather, and ruptured the line, allowing oil at a gauge pressure of 450 psi (30 bar) to escape.

If dead-ends cannot be avoided, they should be connected to the *top* of the main pipeline (unless the liquid in the pipeline is denser than water).

An unusual—and unnecessary—dead-end was a length of 2-in. pipe welded onto a process line to provide a support for an instrument (Figure 9-2). Water collected in the support. Four years after it had been installed, the process line corroded through, and a leak of liquefied gas occurred.

Another serious failure occurred because water in a dead-end was suddenly vaporized. A heavy oil was dried by heating it to 120°C in a tank

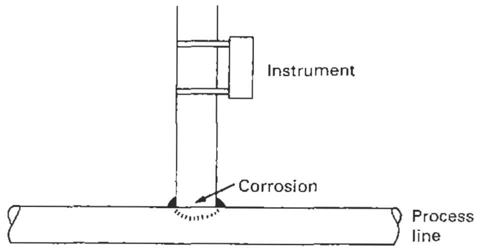


Figure 9-2. Water collected in the instrument support and corroded the process line.

filled with steam coils. The oil was circulated while it was being dried. The suction line projected into the conical base of the tank, forming a dead-end, as shown in Figure 9-3.

As long as the circulation pump was kept running, water could not settle out in the dead-end. The foreman knew the pump had to be kept running. When he was transferred to another plant, this information was lost, and the pump was used only for emptying the tank.

This worked satisfactorily for a time until some water collected in the dead-end and gradually warmed up as the oil was heated. When the temperature reached 100°C, the water vaporized with explosive violence and burst the equipment. The escaping oil caught fire, five men were killed, and the tank ended up in the plant next door.

This incident illustrates the dangers of dead-ends and the pressures developed when water is suddenly vaporized. It also shows how easily knowledge can be lost when people leave. Even if the new foreman was *told* to run the pump all the time or if this was written in the instructions, the reason for doing so might be forgotten, and the circulation might be stopped because it seemed unnecessary or to save electricity.

Other incidents caused by the sudden vaporization of water are described in Sections 12.2 and 12.4.5.

An explosive decomposition in an ethylene oxide (EO) distillation column, similar in its results to that described in Section 7.3.2, may have been set off by polymerization of EO in a dead-end spot in the column base where rust, a polymerization catalyst, had accumulated. Such dead-ends should be avoided. However, it is more likely that a flange leaked; the leaking gas ignited and heated an area of the column above the temperature at which spontaneous decomposition occurs. The source of ignition of the leak may have been reaction with the insulation, as described

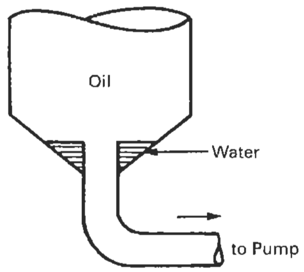


Figure 9-3. Water in this dead-end was vaporized by oil.

in Section 7.3.2. When flange leaks are likely, or their consequences serious, flanges should be left uninsulated [14].

Dead-ends in domestic water systems can provide sites for the growth of the bacteria that cause Legionnaires' disease [15].

Some vertical drain lines in a building were no longer needed, so they were disconnected and capped but left connected to the horizontal main drain below. The caps were fixed with tape but were not made watertight as there was no way, it seemed, that water could get into them. Fifteen years later a choke developed in the main drain, water backed up into the disused legs and dripped into an electrical switch box. All power was lost, and some of the switch gear was damaged beyond repair [23].

9.1.2 Poor Support

Pipes have often failed because their support was insufficient and they were free to vibrate. On other occasions they failed because their support was too rigid and they were not free to expand.

(a) Many small-diameter pipes have failed by fatigue because they were free to vibrate. Supports for these pipes are usually run on-site, and it is not apparent until startup that the supports are inadequate. It is very easy for the startup team, busy with other matters, to ignore the vibrating pipes until the team has more time to attend to them. Then the team gets so used to them that it does not notice them.

Vibration and failure are particularly liable to occur when a small-diameter pipe carries a heavy overhung weight. Within 30 minutes of the start of a new compressor, a pressure gauge fell off for this reason [24].

When equipment receives impulses at its own natural frequency of vibration, excessive vibration (resonance) occurs, and this can lead to rapid failure. A control valve was fitted with a new spindle with slightly different dimensions. This changed its natural frequency of vibration to that of the impulses of the liquid passing through it (the frequency of rotation of the pump times the number of passages in the impeller). The spindle failed after three months. Even a small change in the size of spindle is a modification [24].

(b) A near failure of a pipe is illustrated in Figure 9-4. An expansion bend on a high-temperature line was provided with a temporary

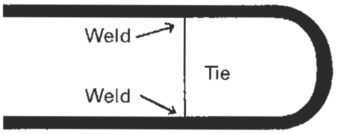


Figure 9-4. A construction support on an expansion bend was left in position.

support to make construction easier. The support was then left in position. Fortunately, while the plant was coming onstream, someone noticed it and asked what it was for.

(c) After a crack developed in a 22-in.-diameter steam main, operating at a gauge pressure of 250 psi (17 bar) and a temperature of 365°C, the main was checked against the design drawings. Many of the supports were faulty. Here's an example from four successive supports:

1. On No. 1 the spring was fully compressed.
2. No. 2 was not fitted.
3. No. 3 was in position but not attached to the pipe.
4. No. 4 was attached, but the nuts on the end of the support rod were slack.

Piping with a 12-in. diameter and larger is usually tailored for the particular duty. There is a smaller factor of safety than with smaller sizes. With these large pipes, it is even more important than with smaller ones that the finished pipework is closely inspected, to confirm that the construction team has followed the designer's instructions.

(d) A pipe was welded to a steel support, which was bolted to a concrete pier. A second similar support was located 2 m away. The pipe survived normal operating conditions. But when it got exceptionally hot, a segment of the pipe was torn out. The fracture extended almost completely around the weld. The bolts anchoring the support to the concrete pier were bent.

This incident was reported in the safety bulletin of another company. The staff members dismissed the incident. "Our design procedures," they said, "would prevent it happening." A little later it did happen. A reflux line was fixed rigidly to brackets welded to the shell of a distillation column. At startup the differential expansion of the hot column and the cold line tore one of the brackets

from the column. Flammable vapor leaked out but fortunately did not catch fire.

(e) A 10-in. pipe carrying oil at 300°C was fitted with a ¾-in. branch on its underside. The branch was located 5 in. from a girder on which the pipe rested. When the pipe was brought into use, the expansion was sufficient to bring the branch into contact with the girder and knock it off. Calculations showed that the branch would move more than 6 in.

(f) On many occasions pipe hangers have failed in the early stages of a fire, and the collapse of the pipes they were supporting has added to the fire. Critical pipes should therefore be supported from below.

(g) An extension was added to a 30-year-old pipebridge that carried pipes containing flammable liquids and gases. To avoid welding, the extension was joined to the old bridge by bolting. Rust was removed from the joining surfaces, and the extension was painted. Water penetrated the crack between the old and new paint and produced rust. As rust is more voluminous than the steel from which it is formed, the rust forced the two parts of the pipebridge apart—a phenomenon known as rust-jacking (see Section 16.3). Some of the bolts failed, and a steam main fractured. Fortunately, the liquid and gas lines only sagged [16].

(h) Eleven pipelines, 2–8 in. (50–200 mm) in diameter, containing hydrocarbon liquids and gases, were supported on brackets of the type shown in Figure 9-5 (a), 2.1 m tall and 6 m apart. The pipes were fixed to two of the brackets and rested on the others. The pipe run passed through a tank farm, and the wind flow through the gaps between the tanks caused the upright part of the supports to incline 2° from the vertical. This was noticed when the pipe run was inspected, but no one regarded it as serious.

As the result of a power failure, the flow through many of the pipes suddenly stopped, and the surge caused the angle of inclination to increase to 6°. The tops of the supports were now 5 in. (125 mm) out of line. The supports were now unstable. Eleven hours after the power failure and three hours after the flows had been restored, the pipe run collapsed over a length of 23 m; 14 tons of gasoline were spilled. Three hours later a further length collapsed. The pipe supports were replaced by the type shown in Figure 9-5 (b).

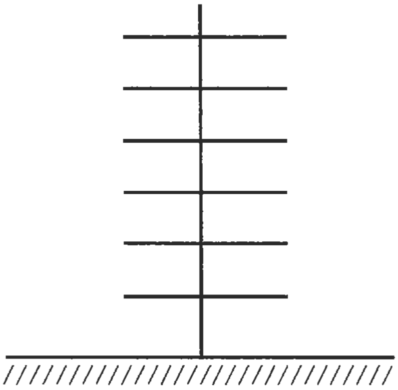


Figure 9-5 (a). The original pipe supports.

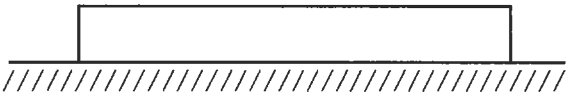


Figure 9-5 (b). The supports used after the collapse.

9.1.3 Water Injection

Water was injected into an oil stream using the simple arrangement shown in Figure 9-6. Corrosion occurred near the point shown, and the oil leak caught fire [5]. The rate of corrosion far exceeded the corrosion allowance of 0.05 in. per year.

A better arrangement is shown in Figure 9-7. The dimensions are chosen so that the water injection pipe can be removed for inspection.

However, this system is not foolproof. One system of this design was assembled with the injection pipe pointing upstream instead of downstream. This increased corrosion.

As discussed in Section 3.2.1, equipment should be designed so that it is difficult or impossible to assemble it incorrectly or so that the incorrect assembly is immediately apparent.

9.1.4 Bellows

Bellows (expansion joints) are a good example of equipment that is intolerant of poor installation or departure from design conditions. They

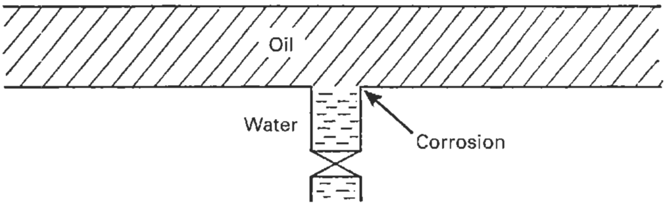


Figure 9-6. Water injection—a poor arrangement.

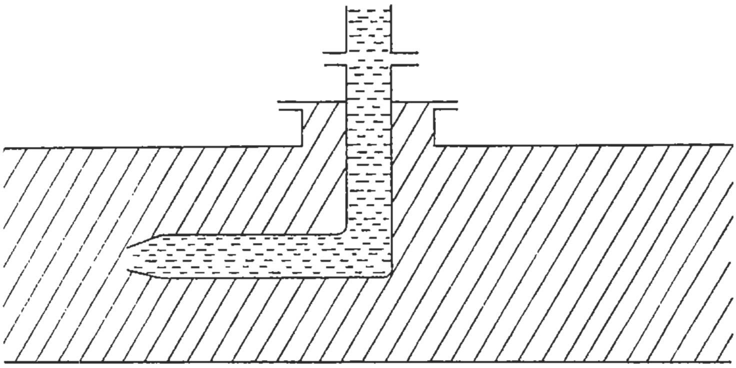


Figure 9-7. Water injection—a better arrangement.

should therefore be avoided on lines carrying hazardous materials. This can be done by building expansion loops into the pipelines.

The most spectacular bellows failure of all time (Flixborough) was described in Section 2.4. Figure 9-8 illustrates a near-failure.

A large distillation column was made in two halves, connected by a 42-in. vapor line containing a bellows. During a shutdown this line was

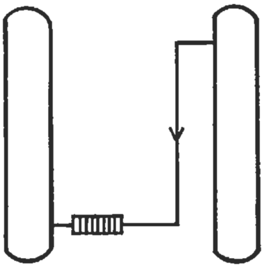


Figure 9-8. A large bellows between the two halves of a distillation column.

steamed. Immediately afterward someone noticed that one end of the bellows was 7 in. higher than the other, although it was designed for a maximum difference of 3 in. Someone then found that the design contractor had designed the line for normal operation. But the design contractor had not considered conditions that might be developed during abnormal procedures, such as startup and shutdown.

9.1.5 Water Hammer

Water hammer (also known as hydraulic shock) occurs in two distinct ways: when the flow of liquid in a pipeline is suddenly stopped, for example, by quickly closing a valve [13], and when slugs of liquid in a gas line are set into motion by movement of gas or condensation of vapor. The latter occurs when condensate is allowed to accumulate in a steam main, because the traps are too few or out of order or in the wrong place. High-pressure mains have been ruptured, as in the following incident.

(a) A 10-in.-diameter steam main operating at a gauge pressure of 600 psi (40 bar) suddenly ruptured, injuring several workers.

The incident occurred soon after the main had been brought back into use after a turnaround. It was up to pressure, but there was no flow along it. The steam trap was leaking and had been isolated. An attempt was made to get rid of condensate through the bypass valve. But steam entered the condensate header, and the line was isolated, as shown in Figure 9-9. Condensate then accumulated in the steam main.

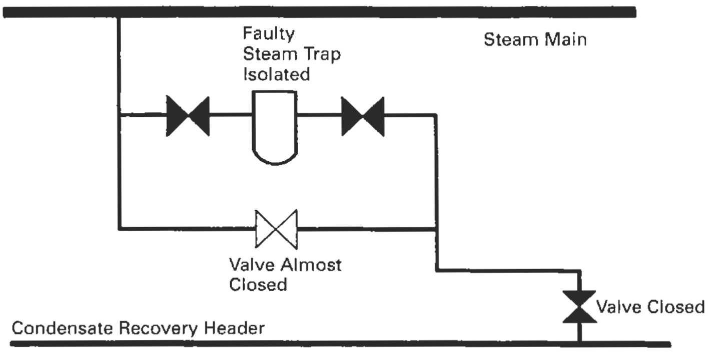


Figure 9-9. Arrangement of valves on steam main that was broken by water hammer.

When a flow was started along the steam main by opening a ¾-in. valve leading to a consuming unit, the movement of the condensate fractured the main [6].

(b) Figure 9-10 shows how another steam main—this time one operating at a gauge pressure of 20 psi (1.4 bar)—was burst by water hammer.

Two drain points were choked and one isolated. In addition, the change in diameter of the main provided an opportunity for condensate to accumulate. The main should have been constructed so that the bottom was straight and so the change in diameter took place at the top.

(c) An operator went down into a pit to open a steam valve that was rarely operated and had been closed for nine months. Attempts to open the valve with a reach rod, 8 m long, had been unsuccessful. The pit was recognized as a confined space, and so the atmosphere was tested, the operator wore a rescue harness, and a stand-by man was on duty outside. The steam main was up to pressure on both sides of the valve, and the gauge pressure was 120 psi (8.3 bar) on the upstream side, 115 psi (7.9 bar) on the downstream side. There was a steam trap on the downstream side of the valve but not on the upstream side, and as the valve was on the lowest part of the system, about 5 tons of cold condensate had accummulated on the upstream side.

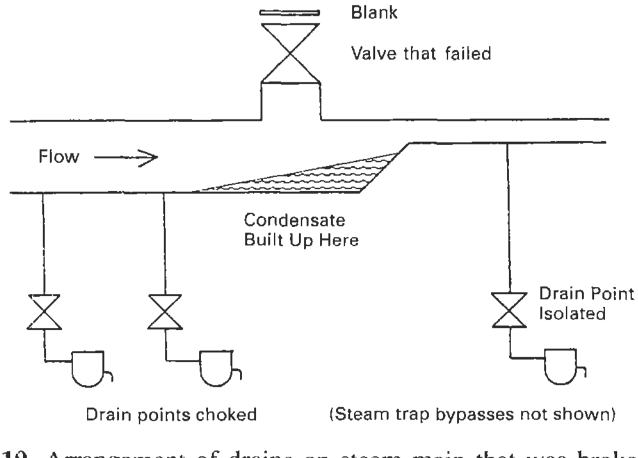
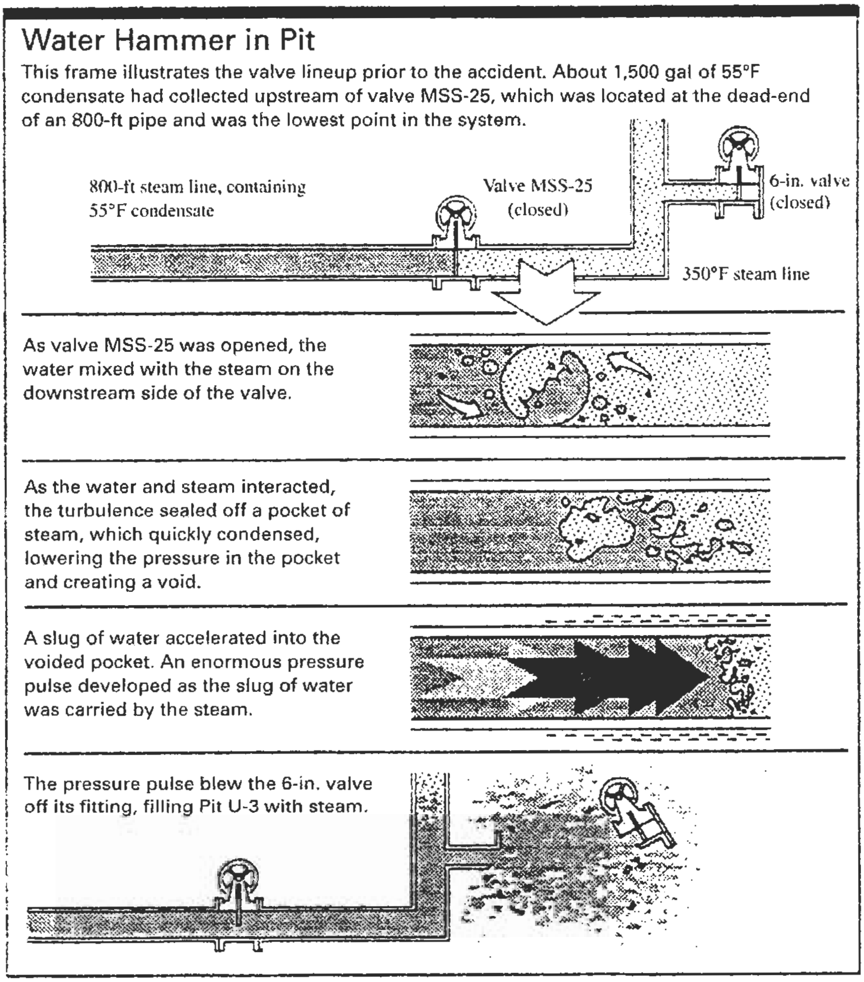


Figure 9-10. Arrangement of drains on steam main that was broken by water hammer.

The operator took about one to two minutes to open the valve halfway; very soon afterward, there was a loud bang as a 6-in. cast-iron valve on a branch (unused and blanked) failed as a result of water hammer. The operator was able to climb out of the pit, but later died from his burns, which covered 65% of his body [17]. Figure 9-11 explains the mechanism.



(Reproduced by permission of the Office of Environment, Safety, and Health, U.S. Department of Energy.)

Figure 9-11. Condensate collected in a steam main. A valve was opened quickly. Sudden movement of the condensate fractured another valve. The figure explains how this occurred.

The accident would not have occurred (or would have been less serious) if:

- Cast iron had not been used. It is brittle and therefore not a suitable material of construction for steam valves, which are always liable to be affected by water hammer.
- There was a steam trap upstream of the valve.
- The valve had been located in a more accessible place.
- The operator had taken longer to open the valve. On previous occasions operators had taken several hours or even longer, but there were no written instructions, and the operator on duty had not been trained or instructed.
- The operating team as a whole had been aware of the well-known hazards of water hammer in steam mains.

For another failure due to water hammer, see Section 10.5.3.

9.1.6 Miscellaneous Pipe Failures

(a) Many failures have occurred because old pipes were reused. For example, a hole 6 in. long and 2 in. wide appeared on a 3-in. pipe carrying flammable gas under pressure. The pipe had previously been used on a corrosive/erosive duty, and its condition was not checked before reuse.

In another case, a 4½-in.-diameter pipe carrying a mixture of hydrogen and hydrocarbons at a gauge pressure of 3,600 psi (250 bar) and a temperature of 350–400°C burst, producing a jet of flame longer than 30 m (Figure 9-12). Fortunately, the pipe was located high up, and no one was injured.

The grade of steel used should have been satisfactory for the operating conditions. Investigation showed, however, that the pipe had previously been used on another plant for 12 years at 500°C. It had used up a lot of its creep life.

Old pipes should never be reused unless their history is known in detail and tests show they are suitable (see Section 9.2.1 h).

(b) Many failures have occurred because the wrong grade of steel was used for a pipeline. The correct grade is usually specified, but the wrong grade is delivered to the site or selected from the pipe store.

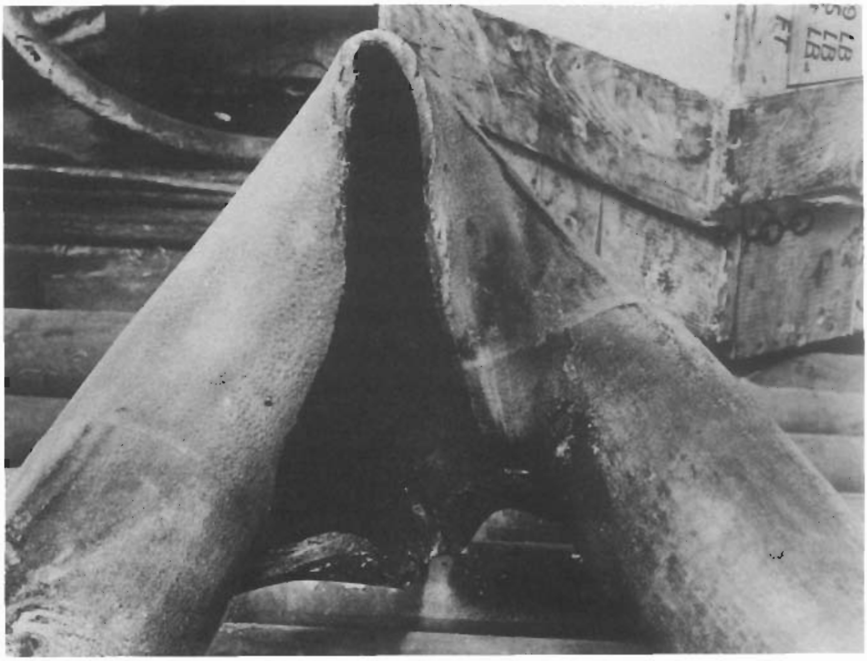


Figure 9-12. An old pipe was reused and failed by creep.

The most spectacular failure of this sort occurred when the exit pipe from a high-pressure ammonia converter was constructed from carbon steel instead of 1¼% Cr, 0.5% Mo. Hydrogen attack occurred, and a hole appeared at a bend. The hydrogen leaked out, and the reaction forces pushed the converter over.

Many companies now insist that if use of the wrong grade of steel can affect the integrity of the plant, all steel must be checked for composition before use. This applies to flanges, bolts, welding rods, etc., as well as the raw pipe. Steel can be analyzed easily with a spectrographic analyzer. Other failures caused by the use of the wrong construction material are described in Section 16.1.

(c) Several pipe failures have occurred because reinforcement pads have been welded to pipe walls, to strengthen them near a support or branch, and the spaces between the pads and the walls were not vented. For example, a flare main collapsed, fortunately while it was being stress-relieved.

Pipe reinforcement pads can be vented by intermittent rather than continuous welding, or a ⅛-in. or ¼-in. hole can be drilled in the pad.

(d) Corrosion—internal or external—often causes leak-before-break failures but not always.

A line carrying liquefied butylene at a gauge pressure of about 30 psi (2 bar) passed through a pit where some valves were located. The pit was full of water, contaminated with some acid. The pipe corroded, and a small leak occurred. The line was emptied for repair by flushing with water at a gauge pressure of 110 psi (7.5 bar). The line was designed to withstand this pressure. However, in its corroded state it could not do so, and the bonnet was blown off a valve. The operator isolated the water. This allowed butylene to flow out of the hole in the pipe. Twenty minutes later the butylene exploded, causing extensive damage [7].

(e) A 1-in. screwed nipple and valve blew out of an oil line operating at 350°C. The plant was covered by an oil mist, which ignited 15 minutes later. The nipple had been installed about 20 years earlier, during construction, to facilitate pressure testing. It was not shown on any drawing, and its existence was not known to the operating team members. If they had known it was there, they would have replaced it with a welded plug.

Similar incidents are described in Section 7.1.5.

(f) Not all pipe failures are due to inadequacies in design or construction (for example, the one described in Section 1.5.2).

A near-failure was also due to poor maintenance practice. A portable, handheld compressed-air grinder was left resting in the space between two live lines. The switch had been left in the On position. So when the air compressor was started, the grinder started to turn. It ground away part of a line carrying liquefied gases. Fortunately the grinder was noticed and removed before it had ground right through the line, but it reduced the wall thickness from 0.28 in. to 0.21 in.

(g) Figure 9-13 shows the pipework on the top of a reactor. When the pipework was cold, any liquid in the branch leading to the rupture disc drained out; when it was hot, it remained in the branch, where it caused corrosion and cracking [18].

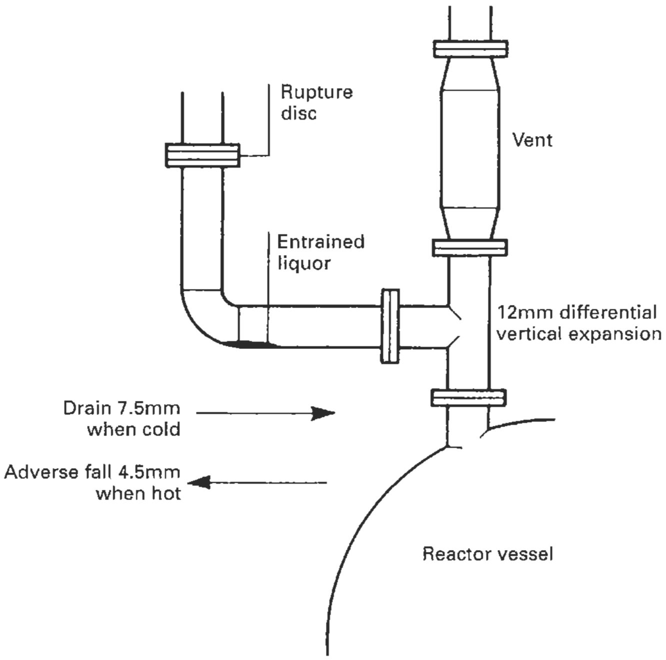


Figure 9-13. The vent arrangements at the top of the reactor. Liquid drained out when the pipework was cold but not when it was hot.

9.1.7 Flange Leaks

Leaks from flanges are more common than those described in Sections 9.1.1–9.1.6 but are also usually smaller. On lines carrying LFGs and other flashing liquids, spiral-wound gaskets should be used in place of compressed asbestos fiber (caf) gaskets because they restrict the size of any leak to a very small value. A section of a caf gasket between two bolts has often blown out, causing a fair-sized leak. But this will not occur with a spiral-wound gasket.

9.1.8 Catastrophic Failures

The fire and explosions in Mexico City in 1984, which killed more than 500 people (see Section 8.1.4), started with a pipe failure. The cause is not known, but the pipe may have been subjected to excessive pressure. Earlier the same year, in February, at least 508 people, most of them children, were killed in Cubatao, Sao Paulo, Brazil, when a 2-ft-diameter

gasoline pipe ruptured and 700 tons of gasoline spread across a strip of swamp. The incident received little publicity, but it seems that, as at Bhopal and Mexico City, a shanty town had been allowed to grow up around the pipeline, on stilts over the swamp. The cause of the failure is not known, but the pipeline was said to have been brought up to pressure in error, and it was also stated that there was no way of monitoring the pressure in the pipeline [10].

9.2 PRESSURE VESSEL FAILURES

Failures of pressure vessels are very rare. Many of those that have been reported occurred during pressure test or were cracks detected during routine examination. Major failures leading to serious leaks are hard to find.

Low-pressure storage tanks are much more fragile than pressure vessels. They are therefore more easily damaged. Some failures are described in Chapter 5.

A few vessel failures and near-failures are described next—to show that they can occur. Failures of vessels as a result of exposure to fire are described in Section 8.1.

9.2.1 Failures (and Near-Failures) Preventable by Better Design or Construction

These are very infrequent.

(a) A leak of gas occurred through the weep hole in a multiwall vessel in an ammonia plant. The plant stayed on line, but the leak was watched to see that it did not worsen. Ten days later the vessel disintegrated, causing extensive damage.

The multiwall vessel was made from an inner shell and 11 layers of wrapping, each drilled with a weep hole. The disintegration was attributed to excessive stresses near a nozzle. These had not been recognized when the vessel was designed.

The report on the incident states: "Our reading of the literature led us to believe that as long as the leaking gas could be relieved through the weep holes, it would be safe to operate the equipment. We called a number of knowledgeable people and discussed the safety issue with them. Consensus at the time supported our conclusion. But after the explosion, there was some dispute over

exactly what was said and what was meant. Knowing what we know now, there can be no other course in the future than to shut down operations in the event of a leak from a weep hole under similar circumstances." [8].

(b) An ammonia plant vessel disintegrated as the result of low-cycle fatigue—the result of repeated temperature and pressure cycles [9].

(c) An internal ball float in a propane storage sphere came loose. When the tank was overfilled, the ball lodged in the short pipe leading to the relief valve, in which it formed an exact fit. When the sphere warmed up, the rise in pressure caused its diameter (14 m) to increase by 0.15 m (6 in.). The increase in diameter was noticed when someone found that the access stairway had broken loose.

A similar incident occurred in a steam drum in which steam was separated from hot condensate. On this occasion, the operator noticed that the pressure had risen above the set-point of the relief valve and tripped the plant [19].

If you use ball-float level indicators, compare the size of the balls with those of the branches on the top of the vessel. If a loose ball could lodge in one of the branches, protect the branch with a metal cage, or use another type of level indicator.

(d) Several vessels have failed, fortunately during pressure testing, adjacent to internal support rings that were welded to the vessel. Expert advice is needed if such features are installed.

(e) N-butane boils at 0°C and iso-butane at −12°C. When the air temperature is below 0°C and a vessel containing butane is being emptied, it is possible to create a partial vacuum and suck in the vessel; this has occurred on several occasions. Vessels used for storing butane and other liquefied gases with boiling points close to 0°C, e.g., butadiene, should be designed to withstand a vacuum. If an existing tank cannot be modified, then warm butane can be recycled, or the butane can be spiked with propane (but the pressure may then be too high in warm weather and the relief valve may lift).

(f) Although I have said that pressure vessel failures are rare, this is not true if vessels are not designed to recognized standards. Davenport [11] has described several liquefied petroleum gas (LPG) vessel failures that were due to poor construction. In the UK in 1984, no one knew who made 30% of the LPG tanks in use, when, or to what standard [12].

(g) The catastrophic failure of a 34-m^3 vessel storing liquid carbon dioxide killed three people, injured eight, caused $20 million damage, and lost three months' production [25]. There were failures by all concerned.

- The vessel was leased from a supplier of carbon dioxide, and the user company did not check that it conformed to the company's usual standards.
- The supplier modified the vessel, but the workmanship was poor. A weld was weak, as it was not full penetration, and brittle because the weld surface, cut with a torch, was not ground before welding.
- As the result of a heater failure, the temperature of the vessel, designed for –29°C, fell to –60°C by evaporative cooling (see Section 10.5.2); at this temperature carbon steel becomes brittle, and cracking may have started.
- Five weeks later the heater failed again, this time in the On position, and the pressure in the tank rose. The two relief valves failed to open because they were fixed to the side of the vessel and connected to the vapor space at the top by an internal line (Figure 9-14)—a most unusual arrangement, presumably adopted so that one nozzle could be used for filling, venting (during filling), and relief. As a result the relief valve was cooled by the liquid in the vessel and became blocked by ice from condensed atmospheric moisture. There was no drain hole in the tailpipe (see Section 10.2.4). The vessel burst, most of the bits ending up in a nearby river, from which they were salvaged.

After the accident a search disclosed 11 other failures that had occurred but had received little or no publicity [26]. If they had been publicized, this incident could have been avoided. The company concerned withdrew all its carbon dioxide vessels that could not withstand low temperatures and replaced them with stainless steel ones. The company found that it could manage with 75% fewer vessels than it had used before (see Section 21.2.1).

At least two of the other 11 failures occurred because the plates from which the vessels were made did not get the correct post-welding heat treatment. Once a vessel has been constructed, it is not easy to check that it has had the correct heat treatment. The

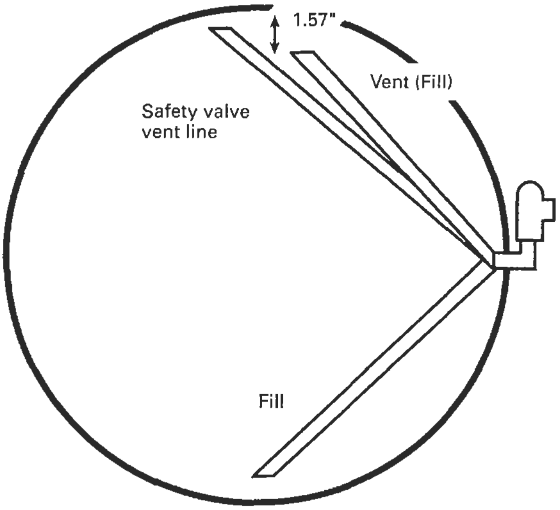


Figure 9-14. Unusual arrangement of relief valve and pipework on tank truck used to transport liquid carbon dioxide. The relief valve was cooled by the liquid and became blocked by ice from condensed atmospheric moisture. *(Illustration courtesy of the Institution of Chemical Engineers.)*

codes do not ask for microscopic examination of the grain structure, but it has been recommended [20].

The main recommendations from the incident were:

- Leased equipment must meet the same standards as all other equipment.
- Do not say, "It must be safe because we are following the regulations and industry standards." They may be out of date or not go far enough.
- Publicizing accidents can prevent them from happening again.

(h) Designers are sometimes encouraged to use second-hand vessels as they are cheaper or immediately available. As with the pipeline in Section 9.1.6 (a), designers should do so only when they know the history of the vessel, including its design code, when they have had it inspected, and when a materials specialist is satisfied that it is suitable for the new duty. The precautions are particularly important (1) when the vessel is intended for use with hazardous materials, (2) at pressures above atmospheric, or (3) at temperatures above or below atmospheric.

At lunch one day, when I worked in industry, I overheard the chief accountant ask a maintenance engineer if he could let him have a length of old rope to make a swing for his daughter. The engineer refused, as he would not, he said, know the history of the rope. (I am aware that in some companies a length of new rope would be declared scrap.)

A centrifuge was offered for sale. Examination showed that a repair to the bowl, by welding, had not been made by the manufacturer but by a contractor.

Old vessels may not be as cheap as they seem at first sight. Nozzles and manways are often in the wrong place, and the cost of modifying them may make the vessel more expensive than a new one. A designer who was persuaded to use an old cylindrical pressure vessel ended up using the two dished ends and nothing more!

Penny-pinching can be tragic, for example, when old tab washers, split pins, and pipes are reused (see Section 16.1 h).

(i) Alert observation can prevent failure. A welder was asked to weld a flange onto a nozzle on a new vessel. He noticed that the weld attaching the nozzle to the tank appeared to be substandard. Thorough examination showed that the seven other nozzle welds on this tank, and several welds on other tanks supplied as part of the same batch, were lacking full penetration along 10–40% of their length [27].

9.2.2 Failures Preventable by Better Operation

The incident described in Section 9.2.1 (a) might be classified as one preventable by better operation of equipment.

(a) Low-pressure storage tanks have often been sucked in, as described in Section 5.3. Pressure vessels can also be sucked in if they have not been designed to withstand vacuum, as the following incident shows.

A blowdown drum was taken out of service and isolated. The drain line was removed and a steam lance inserted to sweeten the tank. The condensate ran out of the same opening.

The condensate was isolated, and 45 minutes later the drain valve was closed. Fifteen minutes later the vessel collapsed. Clearly, 45 minutes was not long enough for all the steam to condense.

(b) A redundant pressure vessel, intended for reuse at atmospheric pressure, had been installed by contractors who decided to pressure-test it. They could not find a water hose to match any of the connections on the vessel. They therefore decided to pressure-test it with compressed air. The vessel reached a gauge pressure of 25 psi (1.7 bar) before it ruptured.

It is possible that the employees concerned did not understand the difference between a pressure test, normally carried out with water, and a leak test, often carried out with compressed air at a pressure well below the test pressure.

This incident shows the need to define the limits within which contractors can work and to explain these limits to contractors' employees.

Another incident in which a pressure vessel was ruptured by compressed air, this time because the vent was choked, is described in Section 2.2 (a).

(c) A vessel, designed to operate at a gauge pressure of 5 psi (0.3 bar) and protected by a rupture disc, was being emptied by pressurization with compressed air. The operator was told to keep the gauge pressure below 5 psi, but he did not do so, and the vessel burst, spraying him with a corrosive chemical. A valve below the rupture disc was closed and had probably been closed for some time.

It is bad practice (and in some countries illegal) to fit a valve between a vessel and its rupture disc (or relief valve). The valve had been fitted to stop escapes of gas into the plant after the disc had blown and while it was being replaced. A better way, if isolation is required, is to fit two rupture discs, each with its own isolation valve, the valves being interlocked so that one is always open.

If compressed gas has to be blown into a vessel that cannot withstand its full pressure, then it is good practice to fit a reducing valve on the gas supply. This would be possible in the case just described. But it may not be possible if the gas is used to blow liquid *into* a vessel. If the gas pressure is restricted to the design pressure of the vessel, it may not be sufficient to overcome friction and change in height.

A sidelight on the incident is that the operator had worked on the plant for only seven months and during that time had received five warnings for lack of attention to safety or plant operations. Howev-

er. the incident was not due to the operator's lack of attention but to the poor design of the equipment. Sooner or later, a valve will be shut when it should be open or vice versa, and the design or method of operation should allow for this (see also Section 1.1 on isolation for maintenance).

(d) Failure of a level controller can allow high-pressure gas to enter a storage tank and rupture it (see Section 5.2.2 c). Pressure vessels have also been ruptured in this way. In one case, gas at a gauge pressure of about 2,200 psi (150 bar) entered a vessel designed for 150 psi (10 bar). Bits of the vessel, up to 2 tons in weight, were found more than 1 km away. The control system was badly designed, as there were two let-down valves in parallel; failure of either could cause rupture of the downstream vessel. In addition, the signals to the two trip valves had been isolated. If the normal control system failed, something we should expect every few years, the only protection was quick action by the operator [21].

(e) A reactor was overpressured by a runaway reaction. Visual examination showed nothing wrong, so the reactor was allowed to continue in service. Eight weeks later it was again overpressured by another runaway reaction, and this time it burst catastrophically. A thorough examination then showed that the reactor had been damaged by the first runaway. (The control instrumentation may also have been damaged, and this may have led to the second runaway.) [28] Equipment that has been taken outside its design or test range should not be used again until it has been examined by a materials expert.

9.2.3 Cylinders

Cylinders have been involved in a number of incidents. The following are typical.

(a) A technician was moving a cylinder containing nitrogen, together with some heavier gas, at a gauge pressure of 600 psi (40 bar). The technician accidentally moved the valve operating lever. The cylinder fell over, and the valve was knocked off. The cylinder then became airborne, hit a platform 6 m above, and went through a sheet metal wall into a building. It went through the roof of this building, 15 m above, and then fell back through the roof and landed 40 m from the point where it had started its journey. Remarkably, no one was injured. Four things were wrong:

- The operating lever should have been removed before the cylinder was moved.
- A safety pin, which would prevent accidental operation, was not in place.
- There was no protective cap over the valve, as this particular design of cylinder was not designed to take one.
- The cylinder should have been moved with a cylinder cart, not by hand.

(b) Several incidents have been due to overfilling. For example, cylinders of uranium hexafluoride (hex) were weighed as they were filled, with the cylinder and the cart that supported it resting on the filling scales. One cylinder was longer than usual. As a result, one wheel of the cart supporting the cylinder overlapped the filling scale and rested on the ground. By the time the operator realized this and moved the cylinder, its weight was above the range of the scales. The operator tried to remove some of the contents of the cylinder by applying a vacuum but without success, probably because some of the hex had solidified. The operator and his supervisor then moved the cylinder into a steam chest and heated it. The contents expanded, and after two hours the cylinder ruptured. One man was killed, and a number injured by the escaping gas. There were many things wrong:

- An operator was asked to fill a cylinder longer than that for which the filling equipment was designed.
- The normal filled weight was close to the top of the scale, so if a cylinder was overfilled, its weight was unknown.
- There was no equipment for emptying overfilled cylinders.
- Although heating overfilled cylinders was against company rules, the operator and his supervisor may not have known this and probably did not understand the reason for the rule [22].

c) A chlorine cylinder was left standing, connected to a regulator, for eight months. The valve became rusted and appeared to be tightly closed though it was not. When someone was disconnecting the regulator, gas spurted into his face. He and three other people who were in the room at the time were hospitalized [29].

REFERENCES

1. J. A. Davenport, *Chemical Engineering Progress,* Vol. 73, No. 9, Sept. 1977, p. 54.
2. T. A. Kletz, *Learning from Accidents,* 2nd edition, Butterworth-Heinemann, Oxford, UK, 1994, Chapter 16.
3. T. A. Kletz, *Plant/Operations Progress,* Vol. 3, No. 1, Jan. 1984, p. 19.
4. U.S. National Transportation Safety Board, *Safety Recommendations,* P-75-14 and 15, 1975.
5. *The Bulletin, The Journal of the Association for Petroleum Acts Administration,* Apr. 1971.
6. *Explosion from a Steam Line: Report of Preliminary Inquiry No. 3471,* Her Majesty's Stationery Office, London, 1975.
7. C. H. Vervalin, *Fire Protection Manual for Hydrocarbon Processing Plants,* Vol. 1, 3rd edition, Gulf Publishing Co., Houston, Texas, 1985, p. 122.
8. L. B. Patterson, *Ammonia Plant Safety,* Vol. 21, 1979, p. 95.
9. J. E. Hare, *Plant/Operations Progress,* Vol. 1, No. 3, July 1982, p. 166.
10. *Hazardous Cargo Bulletin,* June 1984, p. 34.
11. J. A. Davenport, "Hazards and Protection of Pressure Storage of Liquefied Petroleum Gases," *Proceedings of the Fifth International Symposium on Loss Prevention and Safety Promotion in the Process Industries,* Société de Chimie Industrielle, Paris, 1986, p. 22-1.
12. A. C. Barrell, *Hazard Assessment Workshop,* Atomic Energy Authority, Harwell, UK, 1984.
13. D. Clarke, *The Chemical Engineer,* No. 449, June 1988, p. 44.
14. B. E. Mellin, *Loss Prevention Bulletin,* No. 100, Aug. 1991, p. 13.
15. *Loss Prevention Bulletin,* No. 091, Feb. 1990, p. 23.
16. B. M. Hancock, "Preventing Piping Failures," *Safety and Loss Prevention in the Chemical and Oil Processing Industries,* Symposium Series No. 120, Institution of Chemical Engineers, Rugby, UK, 1990, p. 589.

17. *Occupational Safety Observer,* Vol. 2, No. 9, U.S. Dept. of Energy, Washington, D.C., Sept. 1993, p. 1.
18. A. B. Smith, *Loss Prevention Bulletin,* No. 102, Dec. 1991, p. 29.
19. M. L. Griffin and F. H. Gurry, "Case Histories of Some Power- and Control-based Process Incidents," Paper presented at AIChE Loss Prevention Symposium, Houston, Texas, Mar./Apr. 1993.
20. T. Coleman, *The Chemical Engineer,* No. 461, June 1989, p. 29.
21. K. C. Wilson, *Process Safety and Environmental Protection,* Vol. 68, No. B1, Feb. 1990, p. 31.
22. *The Safety of the Nuclear Fuel Cycle,* Organization for Economic Cooperation and Development, 1993, p. 206.
23. *Operating Experience Weekly Summary,* No. 97-32, Office of Nuclear and Facility Safety, U.S. Dept. of Energy, Washington, D.C., 1997, p. 6.
24. F. K. Crawley, *Loss Prevention Bulletin,* No. 134, Apr. 1997, p. 21.
25. W. E. Clayton and M. L. Griffin, *Process Safety Progress,* Vol. 13, No. 4, Oct. 1994, p. 203, and *Loss Prevention Bulletin,* No. 125, Oct. 1995, p. 3.
26. W. E. Clayton and M. L. Griffin, *Loss Prevention Bulletin,* No. 126, Dec. 1995, p. 18.
27. *Operating Experience Weekly Summary,* No. 97-12, Office of Nuclear and Facility Safety, U.S. Dept. of Energy, Washington, D.C., 1997, p. 6.
28. S. J. Brown and T. J. Brown, *Process Safety Progress,* Vol. 14, No. 4, Oct. 1995, p. 245.
29. *Safety Management* (South Africa), Nov./Dec. 1990, p. 45.

Chapter 10

Other Equipment

> Occasionally all the valves on a ring main would be closed and the pressure in a pump rise to danger point. No one appeared to realize that there was anything wrong with this state of affairs.
>
> —A UK gas works in 1916, described by Norman Swindin, *Engineering Without Wheels*

Incidents involving storage tanks, stacks, pipelines, and pressure vessels have been described in Chapters 5, 6, and 9. This chapter describes some incidents involving other items of equipment.

10.1 CENTRIFUGES

Many explosions, some serious, have occurred in centrifuges handling flammable solvents because the nitrogen blanketing was not effective.

In one case a cover plate between the body of the centrifuge and a drive housing was left off. The nitrogen flow was not large enough to prevent air from entering, and an explosion occurred, killing two men. The source of ignition was probably sparking caused by the drive pulley, which had slipped and fouled the casing. However, the actual source of ignition is unimportant. In equipment containing moving parts, such as a centrifuge, sources of ignition can easily arise.

In another incident the nitrogen flow was too small. The range of the rotameter in the nitrogen line was 0–60 L/min (0–2 ft^3/min) although 150 L/min (5 ft^3/min) was needed to keep the oxygen content at a safe level.

On all centrifuges that handle flammable solvent, the oxygen content should be continuously monitored. At the very least, it should be checked every shift with a portable analyzer. In addition, the flow of nitrogen should be adequate, clearly visible, and read regularly.

These recommendations apply to all equipment blanketed with nitrogen, including tanks (Section 5.4) and stacks (Section 6.1). But the recommendations are particularly important for centrifuges due to the ease with which sources of ignition can arise [1].

Another hazard with centrifuges is that if they turn the wrong way, the snubber can damage the basket. It is therefore much more important than with pumps to make sure this does not occur.

One centrifuge was powered by a hydraulic oil installation 2–3 m away. A leak of oil from a cooler was ignited, and the fire was spread by oil and product spillages and by plastic-covered cables. It destroyed the plastic seal between the centrifuge and its exit chute. There was an explosion in the chute and a flash fire in the drier to which it led. The centrifuge exit valve was closed, but the aluminum valve actuator was destroyed. Fortunately, the exit valve did not leak, or several tons of solvent would have been added to the fire. Aluminum is not a suitable material of construction for equipment that may be exposed to fire.

10.2 PUMPS

10.2.1 Causes of Pump Failure

The main cause of pump failure, often accompanied by a leak, are:

(a) Changing the operating temperature or pressure or the composition of the liquid so that corrosion increases. Any such change is a modification and its effects should be reviewed before it is made, as discussed in Chapter 2.

(b) Incorrect installation or repair, especially in fitting the bearings or seals; badly fitted pipework can produce large, distorting forces, and sometimes pumps rotate in the wrong direction.

(c) Maloperation, such as starting a pump before all the air has been removed, starting with the delivery valve open or the suction valve closed, starting with a choked or missing strainer, or neglecting lubrication.

(d) Manufacturing faults: new pumps should be checked thoroughly. Make sure the pump is the one ordered and that the material of construction is the same as that specified (see Section 16.1).

10.2.2 Types of Pump Failure

The biggest hazard with pumps is failure of the seal, sometimes the result of bearing failure, leading to a massive leak of flammable, toxic, or corrosive chemicals. Often it is not possible to get close enough to the pump suction and delivery valves to close them. Many companies therefore install remotely operated emergency isolation valves in the suction lines (and sometimes in the delivery lines as well), as discussed in Section 7.2.1. A check valve (nonreturn valve) in the delivery line can be used instead of an emergency isolation valve, provided it is scheduled for regular inspection.

Another common cause of accidents with pumps is dead-heading—that is, allowing the pump to run against a closed delivery valve. This has caused rises in temperature, leading to damage to the seals and consequent leaks. It has caused explosions when the material in the pump decomposed at high temperature. In one incident, air saturated with oil vapor was trapped in the delivery pipework. Compression of this air caused its temperature to rise above the auto-ignition temperature of the liquid, and an explosion occurred—a diesel-engine effect.

Positive pumps are normally fitted with relief valves. These are not usually fitted to centrifugal pumps unless the process material is likely to explode if it gets too hot. As an alternative to a relief valve, such pumps may be fitted with a high-temperature trip. This isolates the power supply. Or a kick-back, a small-diameter line (or a line with a restriction orifice plate) leading from the delivery line back to the suction vessel, may be used. The line or orifice plate is sized so that it will pass just enough liquid to prevent the pump from overheating. Small-diameter lines are better than restriction orifice plates as they are less easily removed.

Pumps fitted with an auto-start will dead-head if they start when they should not. This has caused overheating. Such pumps should be fitted with a relief valve or one of the other devices just described.

A condensate pump was started up by remote operation, with both suction and delivery valves closed. The pump disintegrated, bits being scattered over a radius of 20 m. If remote starting must be used, then some form of interlock is needed to prevent similar incidents from occurring.

Pumps can overheat if they run with the delivery valve almost closed. In one incident a pump designed to deliver 10 tons/hr was required to deliver only ¼ ton/hr. The delivery valve was gagged, the pump got too hot, the casing joint sprang, and the contents leaked out and caught fire.

If a pump is required to deliver a very small fraction of its design rate, a kick-back should be provided.

Many bearing failures and leaks have occurred as the result of lack of lubrication. Sometimes operators have neglected to lubricate the pumps. On one occasion, a bearing failure was traced to water in the lubricating oil. The bearing failure caused sparks, which set fire to some oily residues nearby. Drums of oil in the open-air lubricating-oil storage area were found to be open so that rainwater could get in. This is a good example of high technology—in bearing and seal design—frustrated by a failure to attend to simple things.

More than any other item of equipment, pumps require maintenance while the rest of the plant is on line. Many incidents have occurred because pumps under repair were not properly isolated from the running plant. See Section 1.1.

10.3 AIR COOLERS

A pump leak caught fire. There was a bank of fin-fan coolers above the pump, and the updraft caused serious damage to the coolers. There was an emergency isolation valve in the pump suction line. This was soon closed and the fire extinguished but not before the fin-fans were damaged. The damage to them was far greater than the damage to the pumps. It is not good practice to locate fin-fans (or anything else) over pumps or other equipment that is liable to leak.

On several other occasions, the draft from fin-fans has made fires worse. And the fans could not be stopped because the Stop buttons were too near the fire. The Stop buttons should be located (or duplicated) at least 10 m away.

Another hazard with air coolers is that even though the motor is isolated, air currents have caused the fans to rotate while they were being maintained. Fans should therefore be prevented from moving before any maintenance work is carried out on or near them.

10.4 RELIEF VALVES

Very few incidents occur because of faults in relief valves themselves. When equipment is damaged because the pressure could not be relieved, someone usually finds afterward that the relief valve (or other relief device) had been isolated (see Section 9.2.2 c), wrongly installed (see Section 3.2.1 e), or interfered with in some other way (see Section 9.2.1 c). The following incidents are concerned with the peripherals of relief valves rather than the valves themselves.

10.4.1 Location

A furnace was protected by a relief valve on its inlet line (Figure 10-1). A restriction developed after the furnace. The relief valve lifted and took most of the flow. The flow through the furnace tubes fell to such a low level that they overheated and burst. The low-flow trip, which should have isolated the fuel supply to the furnace when the flow fell to a low value, could not do so because the flow through it was normal.

The relief valve should have been placed after the furnace or, if this was not possible, before the low-flow trip.

Another point on location that is sometimes overlooked is that most relief valves are designed to be mounted vertically and should not be mounted horizontally.

10.4.2 Relief-Valve Registers

All companies keep a register of relief valves. They test them at regular intervals (every one or two years) and do not allow their sizes to be changed without proper calculation and authorization.

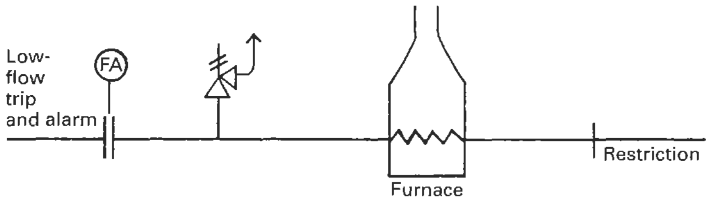


Figure 10-1. When the relief valve lifted, the flow through the furnace was reduced.

However, equipment has been overpressured because the following items were not registered. They had been overlooked because they were not obviously a relief device or part of the relief system.

(a) A hole or an open vent pipe—the simplest relief device possible. Section 2.2 (a) described how two men were killed because the size of a vent hole in a vessel was reduced from 6 in. to 3 in.

(b) A restriction orifice plate limiting the flow into a vessel or the heat input into a vessel should be registered if it was taken into account in sizing the vessel's relief valve.

Restriction plates are easily removed. A short length of narrow diameter pipe is better.

(c) A control valve limiting the flow into a vessel or the heat input into a vessel should be registered if its size was taken into account in sizing the vessel's relief valve. The control valve record sheets or database entries should be marked to show that the trim size should not be changed without checking that the relief valve will still be suitable.

(d) Check (nonreturn) valves should be registered *and inspected regularly* if their failure could cause a relief valve to be undersized. Usually two check valves *of different types* in series are used if the check valve forms part of the relief system.

10.4.3 Changing Relief Valves

Some vessels are provided with two full-size relief valves so that one can be changed with the plant on line. On the plant side of the relief valves, isolation valves are usually provided below each relief valve, interlocked so that one relief valve is always open to the plant (Figure 10-2). If the relief valves discharge into a flare system, it is not usual to provide such valves on the flare side. Instead the relief valve is simply removed and a blank fitted quickly over the end of the flare header before enough air is sucked in to cause an explosion. Later the blank is removed and the relief valve replaced.

On one plant a fitter removed a relief valve and then went for lunch before fitting the blank. He returned just as an explosion occurred. He was not injured by the explosion but was slightly injured sliding down a pipe to escape quickly.

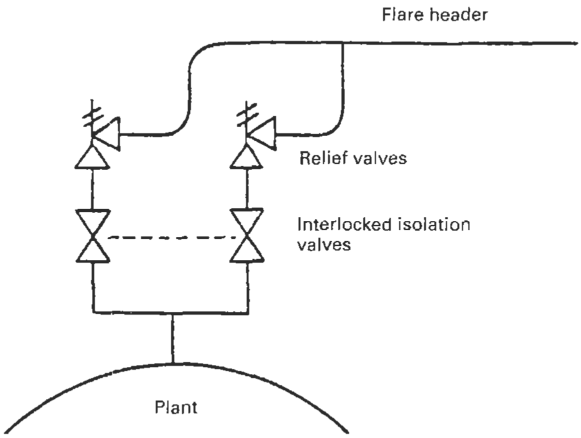


Figure 10-2. Two relief valves with interlocked isolation valves. This figure is diagrammatic. If any liquid might be present, the tailpipe should fall, not rise, after it leaves the relief valve. Otherwise, liquid may collect in the dip and produce a back pressure.

Removing a valve and fitting a blank is satisfactory if the operators make sure, before the relief valve is removed, that the plant is steady and that this relief valve or any other is unlikely to lift. Unfortunately, such instructions may lapse with the passage of time. This occurred at one plant. The people there were fully aware that air might get into the flare system. They knew about the incident just described. But they were less aware that oil might get out. While an 8-in. relief valve was being changed, another relief valve lifted, and gasoline came out of the open end. Fortunately it did not ignite.

The investigation showed that at the time the operating team members were busy at the main plant, which they operated. A deputy foreman had been left in charge of changing the relief valve. He wanted to get it done while a crane was available.

The best way to change a relief valve when a plant is on line is to use the sealing plate shown in Figure 10-3.

All but two of the bolts joining the relief valve to the flare header are removed. The sealing plate is then inserted between the relief valve and the flare header. It is secured by special bolts with small heads that pass through the bolt holes in the relief-valve flange but not through the holes in the sealing plate. The last two bolts can then be removed and the relief valve removed. To replace the relief valve the procedure is reversed [2].

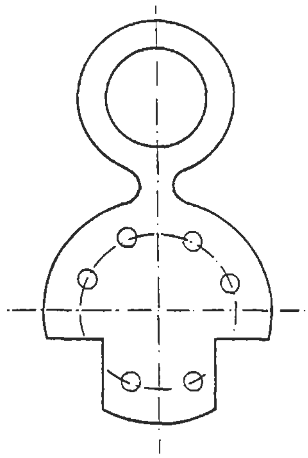


Figure 10-3. Sealing plate for changing relief valves.

This system is recommended for changing relief valves on lines greater than 4 in. diameter.

Flare lines should never be slip-plated with ordinary slip-plates because they may be left in position in error. The sealing plate cannot be left in position when the relief valve is replaced.

When replacing relief valves, care must be taken to make sure that the right relief valve is replaced. Section 6.1 (d) describes another incident that occurred when a flare line was broken. Valves of different internal sizes may look alike (see Section 1.2.4).

10.4.4 Tailpipes

Figure 10-4 shows what happened to the tailpipe of a steam relief valve that was not adequately supported. The tailpipe was not provided with a drain hole (or if one was provided, it was too small), and the tailpipe filled with water. When the relief valve lifted, the water hit the curved top of the tailpipe with great force. Absence of a drain hole in a tailpipe also led to the incident described in Section 9.2.1 (g).

On other occasions, drain holes have been fitted in relief-valve tailpipes even though the relief valve discharged into a flare system. Gas has then escaped into the plant area.

On occasions, relief-valve exit pipes have not been adequately supported and have sagged on exposure to fire, restricting the relief-valve discharge.

Figure 10-4. This relief-valve tailpipe was not adequately supported.

10.4.5 Relief-Valve Faults

Here are a few examples of faults in relief valves themselves. These are not the results of errors in design but of poor maintenance practice. The following have all been seen:

1. Identification numbers stamped on springs, thus weakening them (Figure 10-5).
2. The sides of springs ground down so that they fit.
3. Corroded springs.
4. A small spring put inside a corroded spring to maintain its strength. Sometimes the second spring was wound the same way as the first spring so that the two interlocked (Figure 10-6).
5. Use of washers to maintain spring strength.
6. Welding of springs to end caps (Figure 10-7).
7. Deliberate bending of the spindle to gag the valve (Figure 10-8).
8. Too many coils allowing little, if any, lift at set pressure (Figure 10-9).

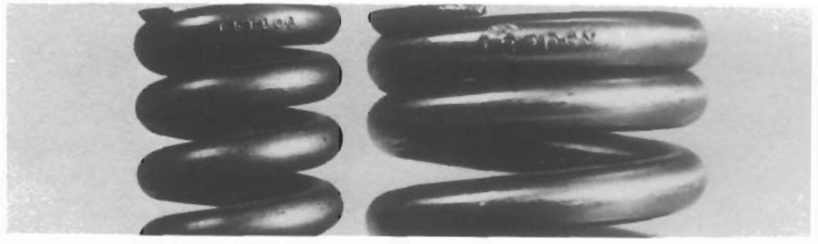


Figure 10-5. Identification marks on body coils could lead to spring failure

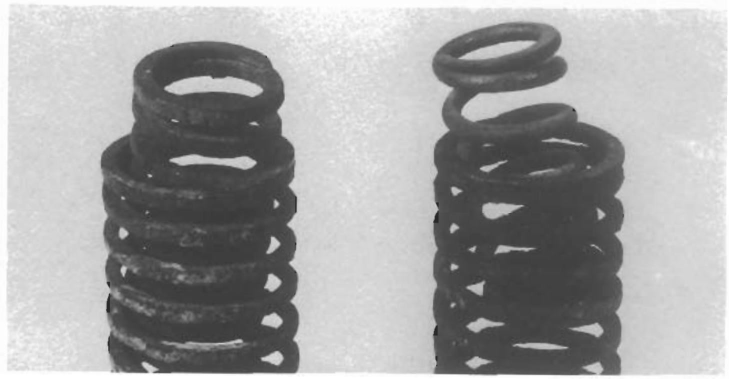


Figure 10-6. Use of additional inner springs of unknown quality in an atten to obtain set pressure.

Figure 10-7. End caps welded to spring. Failure occurred at weld.

Figure 10-8. Deliberate bending of the spindle to gag the valve.

Figure 10-9. Example of too many coils.

Do not assume that such things could not happen in your company (unless you have spent some time in the relief-valve workshop). All relief valves should be tested and inspected regularly. Reference 3 describes model equipment and procedures. When a large petroleum company introduced a test program, it was shocked by the results: out of 187 valves sent for testing, 23 could not be tested because they were leaking or because the springs were broken, and 74 failed to open within 10% of the set pressure—that is, more than half of them could not operate as required [4].

Testing, of course, must be thorough. The following incident is described in the form of a conversation between an inspector investigating a boiler explosion and the maintenance foreman [12].

Inspector: "When was the relief valve last checked?"

Foreman: "After the last overhaul."

Inspector: "How was it checked?"

Foreman: "I set it myself, using the boiler's own pressure gauge."

Inspector: "Why didn't you use a master gauge?"

Foreman: "I didn't need to. The gauge had been checked and found accurate only two weeks before."

Inspector: "Who checked it?"

Foreman: "Mr. X, one of my fitters. He has often done so in the past."

The inspector then spoke to Mr. X.

Inspector: "I understand you checked the pressure gauge two weeks before the explosion."

Mr. X: "Yes, the foreman told me to do so."

Inspector: "When was your master gauge last calibrated?"

Mr. X: "I didn't use one."

Inspector: "You didn't use a master gauge? Then how did you check it?"

Mr. X: "I checked it against the relief valve. I knew it was correct because the foreman told me he had adjusted it himself."

This incident occurred in the 19th century when boiler explosions were much more frequent than they are today. But are you sure something similar could not occur today? Read Sections 10.7.2 (b) and (c) before you decide.

Similar incidents have occurred in technical reports. A writes something in a book or paper. B copies it without acknowledgment. A then repeats it in another report, citing B as the source and thus giving it an authenticity it lacked in its first publication.

10.4.6 Disposal of Relief Discharges

Material discharged from relief valves and rupture discs should not be discharged to atmosphere unless:

- It will have no harmful effects, for example, steam, compressed air, or nitrogen.
- It is a gas at a pressure high enough to disperse by jet mixing. It is necessary to use a pilot-operated relief valve that is either open or shut and is not a type that will hover. Although it is safe to discharge gases such as ethylene and propylene in this way, there may be objections on environmental grounds.
- The amount released is negligible, for example, the relief valves that protect a pipeline that has been isolated.
- A system of trips or interlocks makes the probability that the relief valve will lift very low, say, less than once in 1,000 years for flammable liquids and less than once in 100 years for flammable gases.
- The relief valve will lift only after prolonged exposure of the equipment to fire and will discharge within the fire area so that the discharge will ignite.

Here are some examples of the results of letting relief valves discharge to atmosphere:

- A 6-in. (150-mm) relief valve on a petrochemical plant discharged benzene vapor to atmosphere. It was ignited by a furnace and exploded, rupturing piping, which released more than 100 tons of various flammable liquids. One man was killed, and damage was extensive [5].
- At Seveso in Italy in 1976, a runaway reaction led to the discharge of the reactor contents, including dioxin, a toxic chemical, through a rupture disc direct to the atmosphere. Although no one was killed, many people developed chloracne, an unpleasant skin disease, and an area of about 17 km^2 was made uninhabitable. A catchpot after the relief device would have prevented the reactor contents from reaching the atmosphere. No catchpot was installed as the designers did not foresee that a runaway might occur, although similar runaways had occurred on other plants (see Section 21.2.5) [6].
- Naphtha vapor from a relief valve on a town gas plant in the UK was ignited by a flare stack. The flame impinged on the napththa line, which burst, starting a secondary fire [7].
- A relief valve sprayed liquid into the face of a passing operator with such force that it knocked his goggles off.
- A reaction involving concentrated sulfuric acid was carried out at atmospheric pressure in a vessel with an opening to the atmosphere at the top. When a runaway occurred, acid was ejected over the surrounding area [13].
- The rupture discs on some water compressors were allowed to discharge inside a building as the water was clean. However, by the time it had drained down through several floors to the basement of the building, it had dissolved some solid material that had been spilt on one of the intervening floors and became hazardous. Discs had failed on several occasions, for unknown reasons. Possible causes were vibration, hammer pressure, and low-cycle fatigue.

If, despite my advice, you let relief devices discharge to atmosphere, make sure that if the discharge ignites, the flame will not impinge on other equipment and that no one will be in the line of fire.

10.4.7 Vacuum Relief Valves

Some large equipment, though designed to withstand pressure, cannot withstand vacuum and has to be fitted with vacuum relief valves. These

usually admit air from the atmosphere. If the equipment contains a flammable gas or vapor, then an explosion could occur with results more serious than collapse of the vessel. Experience shows that a source of ignition may be present even though we have tried to remove all possible sources (see Section 5.4). It is therefore better to protect equipment that cannot withstand vacuum by means of a pressure control valve that admits nitrogen or, if nitrogen is not available, another gas such as fuel gas. Very large amounts may be necessary. For example, if the heat input to a large refinery distillation column stopped but condensation continued, 8,000 m^3/hr of gas, the entire consumption of the refinery, would be required. Instead, a much smaller amount was supplied to the inlet of the condenser, thus blanketing it and stopping heat transfer [14]. The simplest solution, of course, is to design equipment to withstand vacuum.

Protection of storage tanks against vacuum is discussed in Sections 5.3 and 5.4.

10.5 HEAT EXCHANGERS

10.5.1 Leaks into Steam and Water Lines

Hydrocarbons can leak through heat exchangers into steam or condensate systems and appear in unexpected places. Some hydrocarbon gas leaked into a steam line that supplied a heater in the basement of a control building. The gas came out of a steam trap and exploded, killing two men. The operators in the control building had smelled gas but thought it had entered via the ventilation system, so they had switched off the fan. The control gear was ordinary industrial equipment, not suitable for use in a flammable atmosphere, and the sparking ignited the gas. It was fortunate that more people were not killed, as the building housed administrative staff as well as operators.

A leak in another heat exchanger allowed flammable gas to enter a cooling-water return line. The gas was ignited by welding, which was being carried out on the cooling tower. The atmosphere had been tested before work started, five hours earlier (see Section 1.3.2).

10.5.2 Leaks Due to Evaporative Cooling

If the pressure on a liquefied gas is reduced, some of the liquid evaporates, and the rest gets colder. All refrigeration plants, domestic and

industrial, make use of this principle. This cooling can affect equipment in two ways: it can make it so cold that the metal becomes brittle and cracks, as discussed in Sections 8.3 and 10.5.2 (g) and it can cause water, or even steam, on the other side of a heat exchanger to freeze and rupture a tube or tubes. The leak that caused the explosion in a control building (see last section) started this way.

Figure 10-10 illustrates another incident. When a plant was shutting down, the flow of cooling water to the tubes of a heat exchanger was isolated. The propylene on the shell side got colder as its pressure fell. The water in the tubes froze, breaking seven bolts. The operators saw ice forming on the outside of the cooler but did not realize that this was hazardous and took no action. When the plant started up again, propylene entered the cooling-water system, and the pressure blew out a section of the 16-in. (400-mm) line. The gas was ignited by a furnace 40 m away, and the fire caused serious damage.

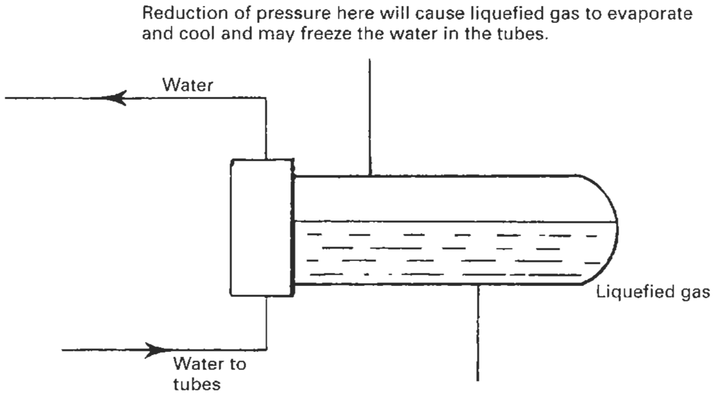


Figure 10-10. Evaporative cooling.

The cooling water should have been kept flowing while the plant was depressured. This would have prevented the water from freezing, provided that depressuring took more than ten minutes.

10.5.3 Damage By Water Hammer

Water hammer (hydraulic shock) in pipelines is discussed in Section 9.1.5. It can also damage heat exchangers, and Figure 10-11 illustrates such an incident.

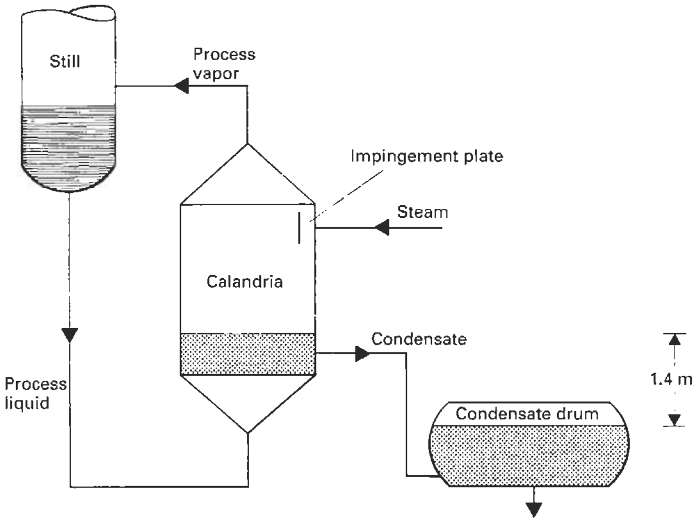


Figure 10-11. Condensate in the steam—the result of too few steam traps—knocked off the impingement plate and damaged the calandria tubes.

The steam supplied to the shell of a distillation column reboiler was very wet, as there was only one steam trap on the supply line although at least three were needed. In addition, condensate in the reboiler drained away only slowly because the level in the drum into which it drained was only 1.4 m below the level in the reboiler.

An impingement plate was fitted to the reboiler to protect the tubes, but it fell off, probably as a result of repeated blows by slugs of condensate. The condensate then impinged on the tubes and squashed or broke 30 of them.

The impingement plate had fallen off several times before and was merely put back with stronger attachments. When something comes apart, we should ask why, not just make it stronger (see Section 1.5.5).

Buildup of condensate in a heat exchanger can cause operating problems as well as water hammer. If the steam supply is controlled by a motor valve and the valve is not fully open, the steam pressure may be too low to expel the condensate, and its level will rise. This will reduce heat transfer, and ultimately the steam supply valve will open fully and expel the condensate. The cycle will then start again. This temperature cycling is bad for the heat exchanger and the plant and may be accompa-

nied by water hammer and corrosion. Proprietary devices are available for overcoming the problem [8].

10.5.4 An Accident During Maintenance

The tube bundle was being withdrawn from a horizontal shell and tube heat exchanger. It was pulled out a few inches and then became stuck. The mechanics decided that the cause was sludge, and to soften it they reconnected the steam supply to the shell. The tube bundle was blown out with some force, causing serious injuries [9].

10.6 COOLING TOWERS

These are involved in a surprisingly large number of incidents; one is described in Section 10.5.1. Wooden packing, after it dries out, is very easily ignited, and many cooling towers have caught fire while they were shut down. For example, the support of a force draft fan had to be repaired by welding. An iron sheet was put underneath to catch the sparks, but it was not big enough, and some of the sparks fell into the tower and set the packing on fire.

Corrosion of metal reinforcement bars has caused concrete to fall off the corners of cooling towers.

A large natural-draft cooling tower collapsed in a 70-mph (110-km/hr) wind, probably due to imperfections in the shape of the tower, which led to stresses greater than those it was designed to take and caused bending collapse [10].

An explosion in a pyrolysis gas plant in Rumania demolished a cooling tower. It fell on the administration block, killing 162 people. Many people who would not build offices close to an operating plant would consider it safe to build them close to a cooling tower. It is doubtful if this is wise.

10.7 FURNACES

10.7.1 Explosions While Lighting a Furnace

Many explosions have occurred while furnaces were being lit. The two incidents described below occurred some years ago on furnaces with simple manual ignition systems, but they illustrate the principles to be followed when lighting a furnace, whether this is carried out manually or automatically.

(a) A foreman tested the atmosphere inside a furnace (Figure 10-12) with a combustible gas detector. No gas was detected, so the slip-plate was removed, and two minutes later, a lighted poker was inserted. An explosion occurred. The foreman and another man were hit by flying bricks, and the brickwork was badly damaged.

The inlet valve was leaking, and during the two minutes that elapsed after the slip-plate was removed, enough fuel gas for an explosion leaked into the furnace. (Suppose the leak was equivalent to a 1.6-mm [1⁄16-in.] diameter hole, and the gauge pressure of the fuel gas was 0.34 bar [5 psi]. The calculation shows that 80 L [3 ft^3] of gas entered the furnace in two minutes. If this burned in 0.01 second, the power output of the explosion was 100 MW.)

The correct way to light a furnace (hot or cold) that burns gas or burns light oil is to start with a positive isolation, such as a slip-plate, in the fuel line. Other positive isolations are disconnected hoses, lutes filled with water (if the fuel is gas at low pressure), and double block and bleed valves; closed valves without a bleed are not sufficient. Then:

1. Test the atmosphere inside the furnace.
2. If no gas is detected, light and then insert the poker (or switch on the electric igniter).
3. Remove the slip-plate (or connect the hose, drain the lute, or change over the double block and bleed valves). If the isolation valve is leaking, the leaking fuel will be ignited by the poker or igniter before it forms an explosive mixture. (The solenoid valve shown in Figure 10-12 should open automatically when the poker is inserted or the igniter is switched on. If it does not, it should be held open until the main burner is lit.)
4. Open the fuel-gas isolation valve.

The furnace had been lit in an incorrect way for many years before the isolation valve started to leak and an explosion occurred. Never say, "It must be safe because we have been doing it this way for years and have never had an accident."

On furnaces with more than one burner, it may be possible to light a burner from another one if the two are close to each other. If they are not, the full procedure just described should be followed. Explosions have occurred on multiburner furnaces because operators assumed that one burner could always be lit from the next one.

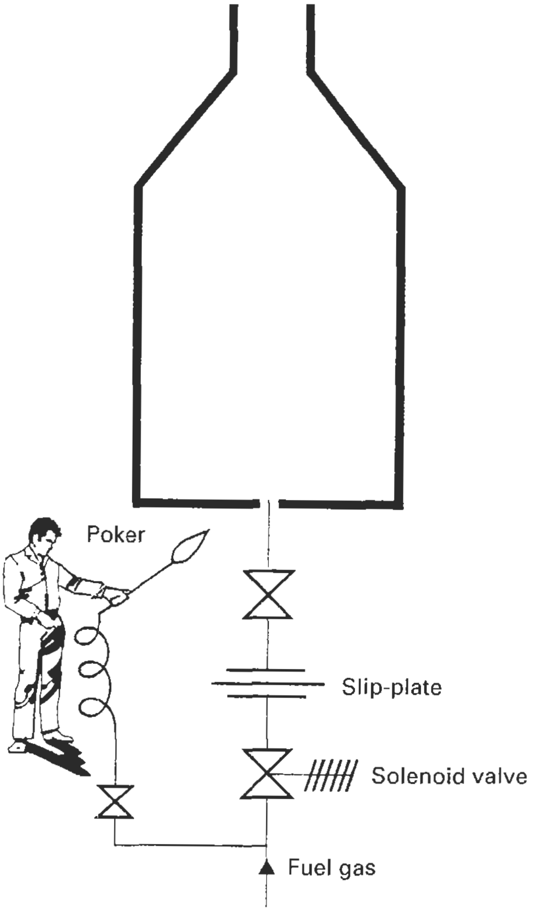


Figure 10-12. Lighting a furnace heated by fuel gas.

(b) A reduction in fuel oil pressure caused the burner in an oil-fired furnace to go out, and the flame failure device closed the solenoid valve in the fuel oil line (Figure 10-13). The operator closed the two hand-isolation valves and opened the bleed between them. (The group of three valves is equivalent to the slip-plate shown in Figure 10-12). When the fuel oil pressure was restored, the foreman tested the atmosphere in the furnace with a combustible gas detector. No gas was detected, so he inserted a lighted poker. The fuel oil supply was still positively isolated, but nevertheless an explosion occurred, and the foreman was injured, fortunately not seriously.

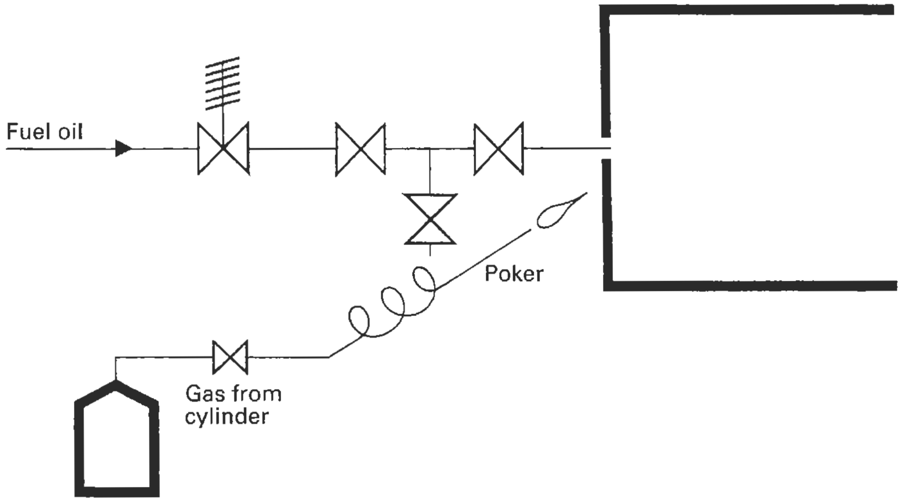


Figure 10-13. Lighting a furnace heated by heavy fuel oil.

When the burner went out, the solenoid valve took a few seconds to close, and during this time some oil entered the furnace. In addition, the line between the last valve and the furnace may have drained into the furnace. The flash point of the fuel oil was 65°C, too high for the oil to be detected by the combustible gas detector. Even though the oil was vaporized by the hot furnace, it would have condensed in the sample tube of the gas detector or on the sintered metal that surrounds the detector head.

Before relighting a hot furnace that burns fuel oil with a flash point above ambient temperature, sweep it out for a period of time, long enough to make sure that any unburnt oil has evaporated. If this causes too much delay, then pilot burners supplied by an alternative supply should be kept alight at all times.

To keep the sweeping-out or purge time as short as possible, the solenoid valve should be close to the burner, and it should close quickly. In addition, the line between the solenoid valve and the burner should not drain into the furnace. As in the previous incident, the furnace had been lit incorrectly for many years before an explosion occurred.

To calculate the purge time:

1. Calculate the amount of oil between the solenoid valve and the burner.

2. Assume it all drains into the furnace and evaporates. Calculate the volume of the flammable mixture, assuming it is at the lower flammable limit, probably about 0.5% v/v. (If it forms a richer mixture, the volume will be less.)
3. Multiply by four to give a safety margin, and sweep out the furnace with this volume of air [11].

10.7.2 Furnace Tube Ruptures

(a) A heat transfer oil was heated in a furnace. A tube in the convection section ruptured along 8 in. (200 mm) of its length, and the ensuing fire damaged three other furnaces. No one could stop the flow of heat transfer oil into the fire, as the valves in the line and the pump switch were too near the furnace. The fire continued until all the oil was burned.

The tube failure was due to prolonged, though not necessarily continuous, overheating of the furnace tubes at times when maximum output was wanted. This led to a creep failure. There were not enough instruments on the furnace to measure the temperature of the tubes, always a difficult problem, and the operators did not understand the way furnace tubes behave. They are usually designed to last for ten years, but if they get too hot, they will not last so long. For instance, if the tubes are designed to operate at 500°C, then:

If they are kept at 506°C they will last 6 years.

If they are kept at 550°C they will last 3 months.

If they are kept at 635°C they will last 20 hours.

If we let the tubes get too hot, however carefully we treat them afterward, they will never be the same again. If we heat them to 550°C, say, for six weeks, we will have used up half their creep life, and they will fail after about five years at design temperature. If we find that our pumps, heat exchangers, and distillation columns will handle a greater throughput than design, we can use it. If we try the same with our furnaces, we may be in trouble in the future.

The following recommendations were made after the fire. They apply to all furnaces.

- Provide good viewing ports. (Although this failure occurred in the convection section of the furnace where the tubes are heated by

hot flue gas, most failures occur in the radiant section as the result of flames impinging on the tubes.)

- Provide tube temperature measurements (but we can never be sure that we are measuring the temperature at the hottest point).
- Train operators in the principles of furnace operation.
- Look for signs of overheating during overhauls.
- Provide remotely operated emergency isolation valves (see Section 7.2.1).
- Provide remote Stop buttons for circulation pumps well away from the furnace.
- Lay out new plants so that circulation pumps are well away from furnaces.
- Do not take a furnace above design output without advice from a materials engineer.
- Examine contractors' proposals critically.

(b) A heat transfer oil was heated in a furnace used only during start-ups to bring reactors up to operating temperature. Startup is always a busy time, and the operator lit the furnace and forgot to open the valves leading from the furnace to the reactors (an example of the sort of lapse of attention we all make from time to time, especially when we are under stress; see Chapter 3). Within 20–30 minutes, a furnace tube ruptured, and there was a large fire with flames 15 m tall.

The furnace was fitted with interlocks that should have isolated the fuel supply if the tube wall temperature or the pressure of the heat transfer oil got too high. Neither interlock worked, and neither had been tested or maintained. The set-point of the high tube wall interlock had been raised far above its original set-point, from 433°C to 870°C, a simple way of putting it out of action [15]. Changing the set-point of an interlock is a modification and should be allowed only when the equipment is capable of withstanding the new conditions (see Chapter 2).

A similar incident occurred on another furnace when the heat transfer oil froze inside the furnace during unusually cold weather. Outside the furnace, the lines were steam-traced. The operating team decided to thaw the frozen oil by lighting one of the burners

in the furnace at a low rate. Later on, someone increased the flow of fuel. About an hour after the furnace was lit, a tube ruptured. There were no instructions on the action to be taken when the oil froze. Lighting a burner had been used before, successfully on that occasion [16].

(c) A feed water pump supplied two boilers. The backup pump also supplied another unit, which was under repair, so the operator on this unit blocked it in. He did not tell the boiler operator what he had done (as in the incident described in Section 17.4).

The on-line feed water pump tripped, but the operator ignored the alarm signal, presumably because he thought the backup pump would start up automatically.

The smaller of the two boilers became short of water first, and the low water level trip shut it down. The operator was so busy trying to get it back on line that he ignored the low water level and other alarms that were sounding on the other boiler. Unfortunately the trips on this boiler did not work, as it had been rewired (incorrectly) since it was last checked. Fifteen to 20 minutes later, someone saw flames coming out of the boiler stack. The boiler was then shut down manually. By this time most of the tubes had melted.

After the furnace had been allowed to cool, the operating team, not realizing the extent of the damage, restarted the flow of feed water. They stopped it when they saw water running out of the firebox. It is fortunate they did not start the water flow earlier, or it would have caused explosive vaporization of the water [17]. As stated in Section 9.2.2 (e), equipment that has been taken outside its design or test range should not be used again until it has been examined.

(d) Another tube failure had an unusual cause. A pipe, sent to an outside workshop for bending, was returned plugged with sand and was welded into the exit line from a furnace. Not surprisingly, the furnace tubes overheated and failed during startup.

The pipe was returned to the plant with a warning that it might contain some sand. The plant staff took this to mean that a few grains might be stuck to the walls, not that the pipe might be full of sand.

Section 14.2.3 describes another failure.

REFERENCES

1. *User's Guide for the Safe Operation of Centrifuges with Particular Reference to Hazardous Atmosphere,* 2nd edition, Institution of Chemical Engineers, Rugby, UK, 1987.
2. T. A. Kletz, *Loss Prevention,* Vol. 6, 1972, p. 134.
3. R. E. Sanders and J. H. Wood, *Chemical Engineering,* Feb. 1993, p. 110.
4. A. B. Smith, *Safety Relief Valves on Pressure Systems,* Reprint No. C454/001/93, Institution of Mechanical Engineers, London, 1993.
5. C. H. Vervalin, *Hydrocarbon Processing,* Vol. 51, No. 12, Dec. 1972, p. 49.
6. T. A. Kletz, *Learning from Accidents,* 2nd edition, Butterworth-Heinemann, Oxford, UK, 1994, Chapter 9.
7. *FPA Journal,* No. 84, Oct. 1969, p. 375.
8. *Loss Prevention Bulletin,* No. 103, Feb. 1992, p. 29.
9. C. Butcher, *The Chemical Engineer,* No. 549, Sept. 16, 1993, p. 24.
10. *Report on the Collapse of the Ardeer Cooling Water Tower, 27 Sept. 1973,* Imperial Chemical Industries Ltd., London, 1974.
11. *Furnace Fires and Explosions,* Hazard Workshop Module No. 005, Institution of Chemical Engineers, Rugby, UK, undated.
12. R. Weaver, *Northern Arrow* (newsletter of the Festiniog Railway Society, Lancashire and Cheshire Branch), No. 147, Oct. 1994.
13. S. J. Brown and T. J. Brown, *Process Safety Progress,* Vol. 14, No. 4, Oct. 1995, p. 244.
14. I. M. Duguid, *Loss Prevention Bulletin,* No. 134, Apr. 1997, p. 10.
15. R. E. Sanders, *Process Safety Progress,* Vol. 15, No. 4, Winter 1996, p. 189.
16. R. E. Sanders, *Management of Change in Chemical Plants—Learning from Case Histories,* Butterworth-Heinemann, Oxford, UK, 1993.
17. S. Mannan, *Process Safety Progress,* Vol. 15, No. 4, Winter 1996, p. 258.

Chapter 11

Entry to Vessels

Many people have been killed or overcome because they entered vessels or other confined spaces that had not been thoroughly cleaned or tested. About 63 people are killed this way every year in the United States; about 40 of those are would-be rescuers (see Section 11.6) [25]. A number of incidents are described here. Another is described in Section 9.1.5 (c), and others involving nitrogen are described in Section 12.3. Sometimes it seems that vessels are more dangerous empty than full.

For further details of the procedures that should be followed when preparing vessels for entry, see References 1 and 2.

11.1 VESSELS NOT FREED FROM HAZARDOUS MATERIAL

In these incidents the vessels were correctly isolated but were not freed from hazardous materials.

(a) A vessel was divided into two halves by a baffle, which had to be removed. The vessel was cleaned out, inspected, and a permit issued for a worker to enter the left-hand side of the vessel to burn out the baffle. It was impossible to see into the right-hand half. But because the left-hand half was clean and because no combustible gas could be detected, it was assumed that the other half was also clean (Figure 11-1). While the welder was in the vessel, some deposit in the right-hand half caught fire. The welder got out without serious injury but bruised himself in his haste.

If a part of the vessel cannot be inspected and be seen to be safe, then we should assume the vessel contains hazardous materials.

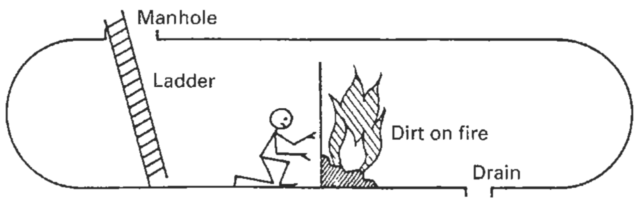


Figure 11-1. If part of a vessel cannot be seen, assume it is dirty.

If the previous contents were flammable, we should assume there is some flammable material out of sight.

If the previous contents were poisonous, we should assume there is some poisonous material out of sight, and air masks should be worn for entry.

Gas tests alone are not conclusive. There may be some sludge present that gives off gas when heated or disturbed.

(b) The last remark is illustrated by the following incidents. To clean a paint-mixing tank, it was washed out with xylene. This cleaned the sides, but some residue had to be scraped from the bottom. While an employee was doing so, wearing neither an air mask nor a lifeline, he was overcome by xylene, which was trapped in the residue and escaped when it was disturbed [3].

A man was overcome by fumes while removing residues from a tank with a high-pressure water jet. When the entry permit was issued, no one realized that fumes might be evolved when the residue was was disturbed [14].

(c) After a permit had been issued to weld inside a vessel, a foreman noticed a deposit on the walls. He scraped some off, tested it, and found that it burned. The permit was withdrawn.

(d) A tank had to be entered for inspection. It had contained only water and was not connected to any other equipment, so the usual tests were not carried out. Three men went into the tank and were overcome. Two recovered but one died. The atmosphere inside the tank was tested afterward and found to be deficient in oxygen. It is probable that rust formation used up some of the oxygen.

Section 5.3 (d) describes how a similar effect caused a tank to collapse.

Although rusting is normally a slow process, it can be rapid under some conditions. Two men collapsed in an evaporator. which had contained warm, moist magnesium chloride. One of them later died. Afterward, tests showed that the oxygen content fell to 1% in 24 hours [9, 10]. Other tests showed that corrosion rates increased ten times when the relative humidity increased from 38% to 52% [11].

Never take shortcuts in entering a vessel. Follow the rules. See also Section 11.6 (b).

(e) Flammable or toxic liquids have been trapped inside the bearings of stirrers and have then leaked out. In one case a worker was overcome while working on a bearing although the vessel had been open for entry for 17 days. He disturbed some trapped liquid. Before issuing an entry permit, look for any places in which liquid might be trapped. Vessels should always be slip-plated as close to the vessel as possible and on the vessel side of isolation valves. Otherwise liquid may be trapped between the valve and the slip-plate. See also Section 11.3 (h).

(f) On several occasions, young, inexperienced workers have been overcome while cleaning tanks. For example, a 16-year-old boy, on his first day at work, was asked to clean out an oil tank with paraffin. He was not supplied with an air mask or protective clothing or given any supervision. He collapsed on the way home from work [12].

(g) A similar incident to (a) occurred in a distillation column filled with a packing made from corrugated and perforated steel sheets. It was cleaned with hot water and steam and opened for inspection. The distributor above the lowest section of packing was found to need repair. A seized bolt was burned off, and part of it fell into the packing, setting it alight. The packing was destroyed. and a 3 m section of the shell had to be replaced.

The material distilled in the column was known to polymerize. but there was no increased pressure drop, and the top of the packing looked clean. so hot work was allowed. If you cannot see that something is clean, assume it is dirty [20].

11.2 HAZARDOUS MATERIALS INTRODUCED

Sometimes, after a vessel has been freed from hazardous materials, they are then deliberately reintroduced, as in the following incidents.

(a) Two men went into a reactor to carry out a dye-penetrant test on a new weld using trichlorethylene. Because the weld was 8 m long, the solvent was soon used up, and the man who was on duty at the entrance was asked to go for some more. He was away for ten minutes. When he returned the two men inside the reactor had collapsed. Fortunately they were rescued and soon recovered.

The amount of solvent that can be taken into a vessel for dye-penetrant testing or other purposes should be limited so that evaporation of the complete amount will not bring the concentration above the safe concentration, for example, the threshold limit value, making allowance for the air flow if the vessel is force-ventilated.

Stand-by workers should not leave a vessel when others are inside it.

(b) A most incredible case has been reported by OSHA [4]. It was decided to shrink-fit a bearing onto a shaft. The shaft was cooled—in a pit—by hosing liquefied petroleum gas onto it while the bearing was heated with an acetylene torch on the floor above the pit. An explosion occurred, killing one man and injuring two others.

(c) The same OSHA report also describes several fatal fires and explosions that occurred while the insides of vessels were being painted, sometimes by spraying. In many cases the "cause" was said to be unsuitable lighting. But people should never be asked to work in a flammable atmosphere in view of the ease with which sources of ignition can turn up. The concentration of flammable vapor should never exceed 20% of the lower flammable limit while people are in a vessel. And if necessary the atmosphere should be monitored continuously. Other fires and explosions were the result of leaks from welding equipment, often ignited when welding started again. Gas tests should always be carried out before welding starts. If oxygen is being used, then the atmosphere should be tested for oxygen as well as flammable vapors.

(d) A small brick-lined reactor, 5 m long by 1.5 m diameter, had to be repaired. The reactor was cleaned, removed from the plant, and taken outside; the bottom pipework and the whole of the reactor top were removed, leaving holes 0.6 m diameter at one end and the full diameter at the other. It was now no more than a length of wide pipeline with a restriction at one end. A man then went inside the reactor to fill in the cracks between the bricks with a rubber adhesive.

The reactor had been repaired in this way many times without incident. One day the weather was very cold, so the reactor was taken indoors. The man repairing the reactor was overcome by the fumes but fortunately soon recovered when he was taken outside [15].

(e) A contractor's employee was repairing the lining of a tank with acetone when it caught fire and he was badly burned. The source of ignition was an unprotected electric light, supplied by the owner of the tank. Both the owner and the contractor were fined; the owner, a much larger firm, was fined ten times as much as the contractor. The judge seemed to consider that the provision of an unprotected light was the major offense, but allowing someone to work in a flammable atmosphere was more serious. This should never be permitted, as a source of ignition is always liable to turn up even though we do what we can to remove known sources [16] (see Section 5.4).

(f) An electrician was working in a pit, using a torch fed by a cylinder of liquefied petroleum gas (LPG), which was standing on the edge of the pit. The hose was rather short, and as a result the electrician pulled the cylinder into the pit. The hose connection next to the cylinder valve broke, and the LPG ignited. The electrician was badly burned [17]. Many accidents have simple causes.

11.3 VESSELS NOT ISOLATED FROM SOURCES OF DANGER

Before entry is allowed into a vessel or other confined space, the vessel should be isolated from sources of hazardous material by slip-plating or physically disconnecting all pipelines and by isolating all supplies of electricity, preferably by disconnecting the cables. On the whole, these precautions seem to be followed. Accidents as the result of a failure to isolate are less common than those resulting from a failure to remove hazardous materials or from their deliberate reintroduction as described in Sections 11.1 and 11.2. However, the following are typical of the accidents that have occurred.

(a) A reactor had been isolated for overhaul. When maintenance was complete, the slip-plates were removed and the vessel prepared for startup. It was then realized that an additional job had to be done, so men were allowed to enter the vessel without the slip-plates being put back and without any gas tests being carried out. An explosion occurred, killing two and injuring two others. It was later found that hydrogen had entered the vessel through a leaking tube [5].

(b) The same report describes a number of incidents in which steam lines failed, as the result of corrosion, while employees were working in a pit or other confined space from which they could not escape quickly. In general, steam lines, heating coils, etc., should be depressured and isolated before entry is permitted to a confined space [6].

(c) On a number of occasions people have been injured because machinery was started up while they were inside a vessel. For example, two men were fixing new blades to the No. 2 unit in a pipe-coating plant. A third man wanted to start up another unit. By mistake he pressed the wrong button. No. 2 unit moved, and one of the workers was killed [7]. The power supply should have been disconnected (see item g).

(d) Contractors were installing a heating coil in a small tank, 2.4 m tall by 1.8 m diameter, which was entered through an opening in the top. A nitrogen line entered the tank, and the nitrogen valve was near the opening. When the job was nearly complete, one of the workmen entered the tank alone. It is believed that while doing so he accidentally knocked the lever-operated valve open, as he was found dead inside the tank, with the nitrogen valve open. The nitrogen supply should have been slip-plated or disconnected. The report said that there were no facilities for isolating the supply, but the valve was not even locked shut [13].

(e) This incident occurred in 1910, but its lessons are still relevant. Two men entered a revolving filter to examine the inside. The inlet line was disconnected, the blow-back gas line was slip-plated, and the 5-in. outlet valve was wide open. Nevertheless the two men were affected by gas but were fortunately able to get out through the manhole.

The liquid, after passing through the outlet valve, joined the line from another filter that was in use. It is believed that carbon dioxide gas from the filter liquid passed up the outlet line into the filter that was being inspected (Figure 11-2). A test showed that "contamination was not sufficient to prevent a candle burning."

The manhole was smaller than those used today, and if the men had been overcome, rescue would have been difficult. Before

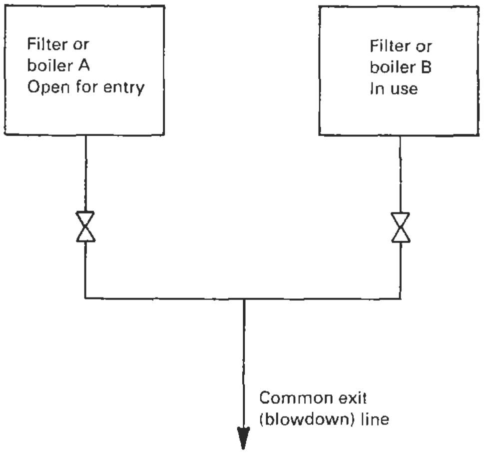


Figure 11-2. Liquid or gas traveled backward from the common line into the vessel that was open for entry.

allowing people to enter a vessel or other confined space, always ask how they will be rescued if they are overcome.

(f) Forty-five years later, in the same company, the accident was repeated, and this time a man was killed. While a man was working inside a boiler, the process foreman noticed that the water level in another boiler was too high. He asked an operator to lower the level through the blowdown (drain) valve, which discharged into a common drain line. Steam entered the boiler under repair from this common line. None of the lines had been slip-plated or disconnected, and the blowdown valve had been left open (Figure 11-2).

To quote from the accident report, "On previous occasions men have entered the boiler without complete isolation. It seems that this first occurred in an emergency when it was thought essential to get a boiler back on line with the minimum of delay, although it is admitted that it does not take long (about 1½ hours) to isolate this type of boiler. Since everything went satisfactorily, the same procedure has apparently been adopted on other occasions, even when, as in this case, there was no particular hurry. Gradually, therefore, the importance of the correct procedure seems to have been forgotten, and on more than one occasion complete reliance seems to have been placed on the presence and reliability of a boiler fitter and his pair of keys. On this occasion, unfortunately, his memory let him down."

The blowdown valves on the boilers were operated by a special key, which had a lug on it so that it could not be removed when the valve was open. It was therefore impossible, in theory, for two blowdown valves to be open at the same time. However, the boiler fitter "kept and jealously guarded" a private key without a lug and had used this one to open the blowdown valve on the boiler that was under repair. He forgot to tell the process foreman what he had done or to close the valve. "The presence of this key would appear to have been of little moment as long as the correct procedure of complete isolation was maintained, but as soon as it was departed from, the additional key became a menace, which eventually enabled the present tragedy to occur," the accident report said.

Any system based on the use of a single key is error prone, as it is so easy to acquire a spare.

(g) Two men were asked to clean out a mixer, which was fitted with large internal mixing blades. Before entering the vessel, they pressed the Start button, as usual, to confirm that the power was isolated. The blades did not move, but the power supply was not isolated; it had failed. The switch was closed, and the fuses had not been removed. When power was restored, the mixer started to turn and both men were killed [18].

Checking the starter before working on electric equipment is a useful final check that should always be made, but it does not prove that the equipment has been isolated; there may be an interruption in the power supply.

(h) A vessel stirrer was fitted with a double mechanical seal supplied with a barrier liquid from a small tank, which was blanketed with nitrogen. The barrier liquid leaked away, and the nitrogen entered the vessel and reduced the oxygen level to 15%. A man who was working in the vessel felt unwell and fortunately left at once.

The atmosphere in the vessel was tested before the man started work, and then a portable blower was installed to keep the atmosphere clean. However, it disturbed the dust produced by grinding, so the man switched it off [19].

11.4 UNAUTHORIZED ENTRY

(a) Contractors unfamiliar with a company's rules have often entered vessels without authority. For example, a contractor's foreman was

found inside a tank, which was disconnected and open, ready for entry, but not yet tested. He had been asked to estimate the cost of cleaning the tank. The foreman said that he did not realize that a permit was needed just for inspection. He had been given a copy of the plant rules but had not read them.

If vessels are open but entry is not yet authorized, the manhole should be covered by a barrier. Do not rely on contractors reading rules. Explain the rules to them.

(b) It is not only contractors who enter vessels without authorization. as shown by Section 11.1 (d) and the following incident.

A process foreman had a last look in a vessel before it was boxed up. He saw an old gasket lying on the floor. He decided to go in and remove it. Everyone else was at lunch, so he decided to go in alone. On the way out, while climbing a ladder, he slipped and fell and was knocked out. His tongue blocked his throat, and he suffocated.

(c) The incident described in Section 12.3.2 (d) shows that you do not have to get inside a confined space to be overcome. Your head is enough. People should never put their heads inside a vessel unless entry has been authorized.

(d) Two teenagers were employed during school holidays as casual laborers at a flour mill, sweeping out wheat left in rail trucks after off-loading. They jumped or fell into a truck before it was empty, were sucked to the base of the truck, became covered in wheat. and were asphyxiated [21].

(e) The most horrendous entry accident I have seen reported occurred in a pulp and paper mill. Two welders were asked to repair the tines in a repulper. This is an open-topped vessel in which large bundles of wood pulp or recycled paper are macerated by a high-energy (40–400 kW) impeller, fitted with tines or blades, to form a 1–5% suspension in water. At 10 a.m. the operators left for a tea break after having drained and cleaned the repulpers. A few minutes later the welders arrived. As No. 3 repulper, the one they had to repair, was clean and empty, they thought it had been cleaned for them and started work.

The operators returned at 10:15 a.m. They saw the welding machine, but the lighting was dim, and they did not see the leads entering the vessel. They filled the vessel with water, turned on the impeller, and fed dry pulp into the vessel.

At 2:30 p.m. the welders were reported missing. Their job card led to No. 3 repulper. It was stopped and drained. Inside were the remains of a rope ladder, welding equipment, and human bones [22].

The welders should have known that they should never enter a vessel until they or their foreman has checked that the vessel is isolated, by slip-plates or disconnection, and has accepted (and signed) an entry permit. Power supplies should have been disconnected, or if merely locked off, each person entering should have added his or her personal lock and kept the key. It is hard to believe that this was the first time normal good practice had not been followed. The management system was at fault.

For another incident, see Section 12.3.2 (f).

11.5 ENTRY INTO VESSELS WITH IRRESPIRABLE ATMOSPHERES

A man was standing on a ladder, ready to go down into a drain manhole to plug one of the inlet lines. The drain contained some hydrogen sulfide, so he had an air mask ready. But he had not yet put it on because he was well outside the manhole. His feet were at ground level (Figure 11-3). He

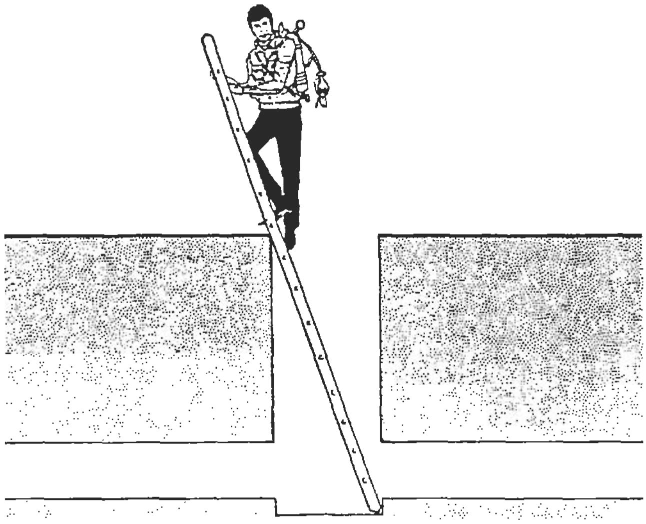


Figure 11-3. A man was overcome by fumes from the manhole.

was about to put on a safety harness when his two companions heard a shout and saw him sliding into the manhole. They were unable to catch him, and his body was recovered from the outfall. He had been overcome by hydrogen sulfide arising from the drains although his face was 1.5 m above ground level.

This incident shows that if a vessel or confined space contains a toxic gas, people can be overcome a meter or more from the opening. Similar incidents involving nitrogen are described in Section 12.3.2 (b).

The incident and the one described in Section 12.3.2 (c) show that special precautions are necessary when entering vessels containing atmospheres that contain so much toxic gas or so little oxygen that there is immediate danger to life. In most cases of entry in which an air mask is worn, it is used because the atmosphere is unpleasant to breathe or will cause harm if breathed for several hours. Only on very rare occasions should it be necessary to enter vessels containing an irrespirable atmosphere. In such cases two persons trained in rescue and resuscitation should be on duty outside the vessel. And they should have available any equipment necessary for rescuing the person inside the vessel, who should always be kept in view.

11.6 RESCUE

If we see another person overcome inside a vessel, there is a very strong natural impulse to rush in and rescue him, even though no air mask is available. Misguided bravery of this sort can mean that other people have to rescue two people instead of one, as shown by the following incidents and by Section 12.3.3.

(a) A contractor entered the combustion chamber of an inert-gas plant while watched by two stand-by men but without waiting for the air masks to arrive. While he was climbing out of the chamber, he lost consciousness halfway up. His body was caught between the ladder and the chamber wall. The stand-by men could not pull him out with the lifeline to which he was attached, so one of them climbed in to try to free him, without an air mask or a lifeline. The stand-by man also lost consciousness. The contractor was finally pulled free and recovered. The stand-by man was rescued by the fire service, but by this time he was dead.

(b) Three men were required to inspect the ballast tanks on a barge tied up at an isolated wharf 20 km from the plant. No tests were carried out. One tank was inspected without incident. But on entering the second tank, the first man collapsed at the foot of the ladder. The second man entered to rescue him and also collapsed. The third man called for assistance. Helpers who were asked to assist in recovering the two men were partly overcome themselves. Representatives of the safety department 20 km away set out with air masks. One man died before he could be rescued.

Tests on other tanks showed oxygen contents as low as 5%. It is believed that rust formation had used up the oxygen, as in the incident described in Section 11.1 (d) [8].

c) Waste zinc cyanide solution dripped into an open-topped tank from equipment that had been electroplated. The tank was about 5 ft by 4 ft by 5 ft deep (1.5 m by 1.2 m by 1.5 m deep) and was located in a building. The liquid had been pumped out, and the next job was to remove sludge from the bottom. An operator sprayed hydrochloric acid into the tank, thus producing hydrogen cyanide, and then went down a ladder into the tank. He was killed, and so were five others who tried to help him. Thirty people were injured, including police and fire fighters called to the scene. No one had any awareness of the hazards. There were no plans for handling emergencies, no one had clearly defined responsibilities, onlookers and relatives milled around, and everyone who entered the building needed medical treatment [23].

It is not clear from the report who authorized the addition of hydrochloric acid and if it had been used before to clean the tank.

(d) A man had to be lowered into a confined space. Great care was taken when choosing the harness, rope, and hoist. The test records were checked to make sure that the equipment chosen had been inspected as required by the company's procedures. But no one noticed that the man put the harness on from back to front. Result: as he was lifted, he could not control his position by holding the rope in front of himself. Instead he hung helpless on the rope, though he came to no harm.

(e) On one occasion a man was locked inside a confined space after his co-workers failed to check that the space was clear before locking the door [25].

11.7 ANALYSIS OF VESSEL ATMOSPHERE

Portable oxygen analyzers that sound an alarm if the oxygen concentration falls are available. They should be carried by all who enter confined spaces, and they could have prevented many of the accidents described in this chapter.

The following incidents show how errors in analysis nearly resulted in people entering an unsafe atmosphere. In both cases the laboratory staff members were asked to test the atmosphere inside a vessel. In the first case they checked the oxygen content with a portable analyzer, in which a sample of the atmosphere being tested is drawn through the apparatus with an aspirator. There was a blockage in the apparatus, so it merely registered the oxygen content of the air already inside it. A bubbler or other means of indicating flow should have been fitted.

In the second case the sample was taken near the manhole instead of being taken near the middle of the vessel. Samples should always be taken well inside the vessel. Long sample tubes should be available so that this can be done. In large vessels and in long, tortuous places like flue gas ducts, samples should be taken at several points.

On both these occasions vigilance by the operating staff members prevented what might have been a serious incident. They suspected something was wrong with the analysis results and investigated the way the samples were taken.

Inevitably, a book like this one is a record of failures. It is pleasant to be able to describe accidents prevented by the alertness of operating staff.

11.8 WHAT IS A CONFINED SPACE?

If we are building a tank or digging a hole in the ground, when does it become a confined space? Guidance is needed. I suggest that when the depth becomes greater than the diameter (and the space is large enough for someone to enter), the space is considered confined. At this time we should consider what precautions, if any, are necessary. In oil and chemical factories, chemicals may drain out of the ground and give off fumes or catch fire; acid has been known to react with limestone in the ground and produce carbon dioxide. On construction sites, the atmosphere in tanks under construction has been contaminated with oxygen or welding gas, or well-meaning fellow workers have connected up nitrogen supplies (see Section 12.3.3).

Section 11.2 (d) describes an incident in which no tests were carried out and the vessel was not recognized as a confined space because ventilation was good. When the vessel was moved indoors, ventilation was no longer good, and a man was overcome.

11.9 EVERY POSSIBLE ERROR

Earlier sections have described how people were killed because vessels were not freed from hazardous materials, atmospheres were not tested and were not respirable, no thought was given to methods of rescue, the correct equipment was not used, or rescue was bungled. This section describes an incident in which all these things were wrong.

A man was asked to clean a 45-m^3 tank that had contained toluene. It was 20 ft (6 m) tall and 10 ft (3 m) diameter. It had not been gas-freed, and the atmosphere had apparently not been tested. He entered the tank through the 16-in.-diameter top opening, using a rope for descent. Self-contained breathing apparatus was available on the job, but he did not wear it. He was overcome by the vapor and lack of air and collapsed on the floor of the tank.

The fire department was called. In an attempt to rescue him, the fire fighters started to cut an opening in the side of the tank. The tank exploded, killing one fire fighter and injuring 15 others. The man who had entered the tank also died, probably from asphyxiation [24].

REFERENCES

1. T. A. Kletz, in D. A. Crowl and S. S. Grossel (editors), *Handbook of Toxic Materials Handling and Management,* Marcel-Dekker, New York, 1994, Chapter 12.
2. F. P. Lees, *Loss Prevention in the Process Industries,* Butterworths, London, 1980, Chapter 21.
3. *Health and Safety at Work,* July 1982, p. 38.
4. W. W. Cloe, *Selected Occupational Fatalities Related to Fire and/or Explosion in Confined Work Spaces as Found in Reports of OSHA Fatality/Catastrophe Investigations,* Report No. OSHA/RP-82/002, U.S. Dept. of Labor, Washington D.C., Apr. 1982, p. 32.
5. Reference 4, p. 22.
6. Reference 4, pp. 65–71.

7. *Occupational Safety and Health,* Supplement, Oct. 1975.
8. *Petroleum Review,* May 1977, p. 49.
9. *Chemical Safety Summary,* Vol. 55, No. 219, Chemical Industries Association, London, 1984, p. 66.
10. R. G. Melchior, *American Industrial Hygiene Association Journal,* Vol. 48, No. 7, 1987, p. 608.
11. *The Sentinel,* Vol. XLIV, No. 2, Industrial Risk Insurers, Hartford, Conn., 2nd quarter 1987, p. 8.
12. *Health and Safety at Work,* Vol. 6, No. 8, Apr. 1984, p. 13.
13. *Chemical Safety Summary,* Vol. 55, No. 219, Chemical Industries Association, London, 1984, p. 63.
14. P. A. Carson and C. J. Mumford, *Loss Prevention Bulletin,* No. 091, Feb. 1990, p. 7.
15. *Loss Prevention Bulletin,* No. 110, Apr. 1993, p. 8.
16. *Health and Safety at Work,* Vol. 15, No. 5, May 1993, p. 9.
17. *Safety Management* (South Africa), Vol. 16, No. 9, Sept. 1990, p. 79.
18. *Safety Management* (South Africa), Vol. 16, No. 4, Apr. 1990, p. 24.
19. *Loss Prevention Bulletin,* No. 112, Aug. 1993, p. 20.
20. *Loss Prevention Bulletin,* No. 122, Apr. 1995, p. 7.
21. *Occupational Safety and Environmental News* (South Africa), Vol. 2, No. 1, 1996, p.1.
22. *Safety Management* (South Africa), Apr. 1997, p. 36.
23. *Occupational Safety and Health Observer,* Vol. 3, No. 10, U.S. Dept. of Energy, Washington, D.C., Oct. 1994, p. 2.
24. An OSHA report quoted in *Operating Experience Weekly Summary,* No. 97-40, Office of Nuclear and Safety Facility, U.S. Dept. of Energy, Washington, D.C., 1997, p. 7.
25. *Operating Experience Weekly Summary,* No. 97-46, Office of Nuclear and Safety Facility, U.S. Dept. of Energy, Washington, D.C., 1997, p. 5.

Chapter 12

Hazards of Common Materials

This chapter is not concerned with the hazards of obviously dangerous materials, such as highly flammable liquids and gases, or toxic materials. Rather, the focus is on accidents involving those common but dangerous substances: air, water, nitrogen, and heavy oils.

12.1 COMPRESSED AIR

Many operators find it hard to grasp the power of compressed air. Section 2.2 (a) describes how the end was blown off a pressure vessel, killing two men, because the vent was choked. Compressed air was being blown into the vessel, to prove that the inlet line was clear. It was estimated that the gauge pressure reached 20 psi (1.3 bar) when the burst occurred. The operators found it hard to believe that a pressure of "only twenty pounds" could do so much damage. Explosion experts had to be brought in to convince them that a chemical explosion had not occurred.

Unfortunately, operators often confuse a force (such as 20 lbs) with a pressure (such as 20 psi) and forget to multiply the 20 lbs by the number of square inches in the end of the vessel.

Section 13.5 describes a similar accident, while Section 5.2.2 describes other incidents in which equipment was damaged by compressed air. Because employees do not always appreciate the power of compressed air, it has sometimes been used to remove dust from workbenches or clothing. Consequently, dust and metal splinters have been blown into people's eyes or into cuts in the skin. Worse still, compressed air has been

used for horseplay. A man was killed when a compressed air hose was pushed up his rectum [1].

Fires have often occurred when air is compressed. Above 140°C, lubricating oil oxidizes and forms a carbonaceous deposit on the walls of air compressor delivery lines. If the deposit is thin, it is kept cool by conduction through the pipework. But when deposits get too thick, they can catch fire. Sometimes the delivery pipe has gotten so hot that it has burst or the aftercooler has been damaged. In one case the fire vaporized some of the water in the aftercooler and set up a shock wave, which caused serious damage to the cooling-water lines.

To prevent fires or explosions in air compressors:

1. Keep the delivery temperature below 140°C. It is easier to do this if the inlet filters are kept clean and the suction line is not throttled. On some rotary air compressors, a large oil surface is exposed to the air, deposits readily form and ignite, and the temperatures should be kept lower.
2. Install a high-temperature alarm or trip on the delivery line.
3. Avoid long periods of operation at low rate, as this can increase oil deposition.
4. Avoid traps in the delivery pipework in which oil can collect.
5. Clean the pipework regularly so that deposits do not get more than ⅛ in. (3 mm) thick. One fire occurred in a compressor on which it was impossible to clean the pulsation dampers.
6. Use special lubricants that reduce the formation of deposits.
7. Use nonlubricated compressors. However, oil is still needed for bearings and gear boxes and may leak into the compressors unless special attention is paid to their design and maintenance [19].

After passing through the aftercooler, the compressed air is usually too cool for deposits to form or catch fire but not always. On one plant an instrument air drier became contaminated with oil and caught fire during the drying cycle.

One company experienced 25 fires or explosions in air-compressor discharge pipework within 35 years. In one of the worst, the fire heated the air going forward into an air receiver, which was lined with bitumen to prevent corrosion. On heating, the bitumen gave off flammable vapors, which exploded, toppling the receiver and demolishing part of a building.

Thin films of oil in pipework can explode without a previous fire if subjected to sudden shock, for example, by rapid opening of a valve [20].

Unexpected concentration of oxygen can occur when compressed air is dried or purified by passing it over certain types of molecular sieves. Nitrogen is absorbed preferentially after regeneration, and the air first produced may be rich in oxygen. This can widen flammability limits and lower auto-ignition temperatures. At least one explosion has occurred as a result. If possible, use Type 3A molecular sieves [21].

Another hazard of compressed air is that it contains dust (organic and inorganic), water, and traces of hydrocarbons, which if they are not removed can cause excessive wear of tools or contamination of products. Morris writes, "Those who use air for pneumatic tools or even paint spray seem to have an inbuilt resistance to any idea that the quality of their compressed air is of any serious consequence. The fact that it transmits concentrated quantities of abrasive particles and water into the finely machined orifices and cylinders of their tools seems to pass them by" [12].

At one time it was believed that hydrocarbon vapor and air in the form of a foam could not explode, and it was even suggested that tanks containing flammable vapor could be made safe for welding or other hot work by filling them with fire-fighting foam. It is now known that this is incorrect and that such foams can explode. In fact, a method proposed for exploding antipersonnel mines laid during the Falkland Islands War is to cover the ground with foam, with a hydrocarbon-air mixture in the bubbles, and then ignite it [13]. (Tanks can, of course, be made safe for welding by filling them with foam made from nitrogen instead of air. This method is often used if the tank contains openings through which nitrogen gas would rapidly disperse.)

Other hazards of compressed air are described in Reference 2.

12.2 WATER

The hazards of water hammer are described in Section 9.1.5 and the hazards of ice formation in Section 9.1.1. This section describes some accidents that have occurred as the result of the sudden vaporization of water, incidents known as boilovers, slopovers, foamovers, frothovers, or puking. Boilover is used if the tank is on fire and hot residues from the burning travel down to the water layer. Slopover is often used if water from fire hoses vaporizes as it enters a burning tank. Sections 9.1.1 and 12.4.5 describe incidents in which vessels burst because water that had

collected in a trap was suddenly vaporized. But most slopovers have occurred when a water layer in a tank was suddenly vaporized, as in the following incidents:

(a) Hot oil, the residue from a batch distillation, was being moved into a heavy residue storage tank. There was a layer of water in the tank—the result of steaming the oil transfer line after previous movements—and this vaporized with explosive violence. The roof of the tank was lifted, and structures taller than 20 m were covered with black oil. A man who saw the incident said the tank exploded, though the sudden release of energy had a physical rather than a chemical cause.

To prevent similar incidents from happening, if heavy oil is being transferred into a tank, incoming oil should be kept *below* 100°C, and a high-temperature alarm should be installed on the oil line. Alternatively, water should be drained from the tank, the tank kept *above* 100°C, and the tank contents circulated before the movement of oil into the tank starts. In addition, the movement of oil into the tank should start at a low rate.

(b) In other cases a water layer has vaporized suddenly when it was heated by conduction from a hotter oil layer above. For example, to clean a tank that had contained heavy oil, some lighter oil was put into it and heated by the steam coil. There was a layer of water below the oil. The operators were told to keep the temperature of the oil below 100°C. But they did not realize that the height of the thermocouple (1.5 m) was above that of the top of the oil (1.2 m). Although the thermocouple was reading 77°C, the oil was above 100°C, the water vaporized, and the roof was blown off the tank.

As the water started to boil and lift up the oil, the hydrostatic pressure on the water was reduced, and this caused the water to boil with greater vigor.

(c) Some paraffin that had been used for cleaning was left in a bucket. There was some water under the paraffin. Some hot equipment set fire to some cleaning rags, and the fire spread to the paraffin in the bucket.

To put out the fire, a man threw a shovelful of wet scale into the bucket. The water became mixed with the oil, turned to steam, and blew the oil over the man, who was standing 1–2 m away. He died from his burns.

1. Never mix water and hot oil.
2. Do not use flammable solvents for cleaning.
3. Do not carry flammable liquids in buckets. Use a closed can (see Section 7.1.3).

Water can be trapped behind heat exchanger baffles and then suddenly vaporized by circulation of hot oil. It can also be trapped in dead-ends and U-bends in pipework (see Section 9.1.1). Such U-bends can form when one end of a horizontal pipe is raised by thermal expansion. The trays in a distillation column were damaged during startup when hot gas met water, from previous steaming, dripping down the column [3]. Section 17.12 describes an incident somewhat similar to a foamover.

Accidents have occurred because hot water was not treated with respect. Five men were killed when a plastic hot-water tank split along a seam [14]. On another plant, a man, about to make some tea, caught his sleeve on the tap of an electric water heater. The heater fell over, 2 gal of hot water fell on him, and he died in the hospital five days later [15]. The heater should have been fixed to the wall. If it had contained a hazardous chemical, it would have been secured, but no one thought hot water was hazardous. Chemicals are not the only hazards on a plant.

Other hazards of water are described in Reference 3.

12.3 NITROGEN [4]

Nitrogen is widely used to prevent the formation of flammable mixtures of gas or vapor and air. Flammable gases or vapors are removed with nitrogen before air is admitted to a plant, and air is removed with nitrogen before flammable gases or vapors are admitted.

There is no doubt that without nitrogen (or other inert gas) many more people would be killed by fire or explosion. Nevertheless we have paid a heavy price for the benefits of nitrogen. Many people have been asphyxiated by it. In one group of companies in the period 1960–1978, 13 employees were killed by fire or explosion, 13 by toxic or corrosive chemicals, and 7 by nitrogen. It is our most dangerous gas.

This section describes some accidents in which people were killed or overcome by nitrogen. Some of the accidents occurred because nitrogen was used instead of air. In others people were unaware of the dangers of nitrogen or were not aware that it was present.

The name *inert gas,* often used to describe nitrogen, is misleading. It suggests a harmless gas. Nitrogen is not harmless. If people enter an atmosphere of nitrogen, they can lose consciousness, without any warning symptoms or distress, in as little as 20 seconds. Death can follow in three or four minutes. A person falls, as if struck down by a blow on the head. In German, nitrogen is known as stickstoff ("suffocating gas"). Perhaps we would have fewer incidents if we called it choking gas instead of inert gas.

12.3.1 Nitrogen Confused With Air

Many accidents have occurred because nitrogen was used instead of compressed air. For example, on one occasion a control room operator noticed a peculiar smell. On investigation it was found that a hose, connected to a nitrogen line, had been attached to the ventilation intake. This had been done to improve the ventilation of the control room, which was rather hot. On other occasions nitrogen has been used by mistake to freshen the atmosphere in vessels in which employees were working. And in another incident, nitrogen was used by mistake to power an air-driven light, used during entry to a vessel. In this case the error was discovered in time. More serious are incidents in which nitrogen has been connected to air masks.

To prevent these errors, many companies use different fittings for compressed air and nitrogen. Nevertheless, confusion can still occur, as the following story shows:

An operator donned a fresh-air hood to avoid breathing harmful fumes. Almost at once he felt ill and fell down. Instinctively he pulled off the hood and quickly recovered. It was then found that the hood had been connected by mistake to a supply of nitrogen instead of compressed air.

Different connections were used for nitrogen and compressed air, so it was difficult at first to see how a mistake had been made. However, the place where the man was working was a long way from the nearest compressed air connection, so several lengths of hose had to be joined together. This was done by cutting off the special couplings and using simple nipples and clamps. Finally, the hoses were joined to one projecting through an opening in the wall of a warehouse. The operator then went into the warehouse, selected what he thought was the other end of the projecting hose and connected it to the air line. Unfortunately, there were sev-

eral hoses on the floor of the warehouse, and the one to which he had joined the air line outside was already connected to a nitrogen line.

To prevent incidents similar to those described, we should:

1. Use cylinder air for breathing apparatus.
2. Label all service points.
3. Use different connections for air and nitrogen and publicize the difference so that everyone knows.

Another incident occurred on a plant where the pressure in the instrument air system was maintained with nitrogen when the instrument air compressor failed. Two operators who were required to wear air masks attached them to the instrument air system. Unknown to them, the compressor had broken down, and the system was full of nitrogen. They both died [16].

A third incident occurred at a U.S. government facility. An employee connected his air mask onto a nitrogen line and immediately blacked out, fell, and hit his head. Fortunately, a stand-by man came to his assistance, and he recovered without serious injury. The compressed air and nitrogen lines used the same couplings, and the nitrogen lines, which should have been a distinctive color, had not been painted [22].

When possible, air from cylinders or a dedicated system should be used instead of general-purpose compressed air. If the latter has to be used, it should be tested at the point of use immediately before use, every time.

12.3.2 Ignorance of the Dangers

(a) A member of a cleaning crew decided to recover a rope, which was half inside a vessel and was caught up on something inside. While kneeling down, trying to disentangle the rope, he was overcome by nitrogen. Afterward he admitted that if necessary he would have entered the vessel.

(b) On several occasions people who were working on or near leaky joints on nitrogen lines have been affected. Although they knew nitrogen is harmful, they did not consider that the amount coming out of a leaky joint would harm them (Figure 12-1).

Two maintenance workers had just removed the cover from a manhole near the top of a distillation column, which had been

Figure 12-1.

swept out with nitrogen, when one of them collapsed. The other pulled him free, and he soon recovered. The bottom manhole had already been removed, and it seems that a chimney effect caused nitrogen to come out of the upper manhole [23].

(c) Two men without masks were killed because they entered a vessel containing nitrogen. Possibly they had removed their masks on other occasions, when the atmosphere was not harmful to breathe, for a moment or two and did not appreciate that in a 100% nitrogen atmosphere they would be overcome in seconds. It is believed that one man entered the vessel, removed his mask, and was overcome and that the second man then entered, without a mask, to rescue him.

Entry should not normally be allowed to vessels containing irrespirable atmospheres. Special precautions are necessary if entry is permitted (see Section 11.5).

(d) You do not have to get right inside a confined space to be overcome. Your head is enough.

When a plant was being leak-tested with nitrogen after a shutdown, a leak was found on a manhole joint on the side of a vessel. The pressure was blown off, and a fitter was asked to remake the

joint. While he was doing so, the joint ring fell into the vessel. Without thinking, the fitter squeezed the upper part of his body through the manhole so that he could reach down and pick up the joint. His companion saw his movements cease, realized he was unconscious, and pulled him out into the open air, where he soon recovered.

(e) In another incident the cover of a large converter was removed, but nitrogen was kept flowing through it to protect the catalyst. An inspector did not ask for an entry permit, as he intended only to "peep in." Fortunately someone noticed that he had not moved for a while, and he was rescued in time.

(f) A contract welder was asked to repair some cracks near the manhole on top of a vessel that had been swept out with nitrogen. To gain access, he removed the plastic sheet that covered the open manhole and placed a ladder inside the vessel, protruding through the manhole. He then stood on the ladder, in a position similar to that shown in Figure 11-3. He dropped the tip of his torch into the vessel, went part way down the ladder to see if he could see it, and collapsed. By the time he was rescued, he was dead [24].

As stated in Section 11.4, if a manhole has been removed but entry has not been authorized, the manhole should be covered by a fixed barrier, not just a plastic sheet. A ladder inside a manhole that is protected by only a loose cover is almost an invitation to enter.

12.3.3 Nitrogen Not Known to Be Present

Some of the incidents described in Section 12.3.2 may fall into this category. Most of the incidents of this type, however, have occurred during construction when one group of workers has, unknown to others, connected up the nitrogen supply to a vessel. The following is an account of a particularly tragic accident of this type.

Instrument personnel were working inside a series of new tanks, installing and adjusting the instruments. About eight weeks earlier, a nitrogen manifold to the tanks had been installed and pressure-tested; the pressure was then blown off and the nitrogen isolated by a valve at the plant boundary. The day before the accident, the nitrogen line was put back up to pressure because the nitrogen was required on some of the other tanks.

On the day of the accident, an instrument mechanic entered a 2-m^3 tank to adjust the instruments. There was no written entry permit because the people concerned believed, mistakenly, that entry permits were not required in a new plant until water or process fluids had been introduced. Although the tank was only 6 ft tall and had an open manhole at the top, the mechanic collapsed. An engineer arrived at the vessel about five minutes later to see how the job was getting on. He saw the mechanic lying on the bottom, climbed in to rescue him, and was overcome as soon as he bent down.

Another engineer arrived after another five or ten minutes. He fetched the process supervisor and then entered the vessel. He also collapsed. The supervisor called the plant fire service. Before they arrived the third man recovered sufficiently to be able to climb out of the vessel. The second man was rescued and recovered, but the first man died. It is believed that an hour or two before the incident, somebody opened the nitrogen valve leading to the vessel and then closed it.

What can we learn from this incident?

1. If someone is overcome inside a vessel or pit, we should never attempt to rescue him without an air mask. We must curb our natural human tendency to rush to his aid, or there will be two people to rescue instead of one (see Section 11.6).
2. Once a vessel has been connected up to any process or service line, the full permit-to-work and entry procedure should be followed. In the present case, this should have started eight weeks before the incident. And the nitrogen line should have been disconnected or slip-plated where it entered the vessel.

   There should be a formal handover from construction so that everyone is aware when it has taken place. The final connection to process or service lines is best made by plant fitters rather than by the construction team. In each plant, the procedure for handover should be described in a plant instruction.
3. When the plant is still in the hands of construction, the normal permit-to-work procedure is not necessary, but an entry permit system should be in force. Before anyone enters a vessel, it should be inspected by a competent, experienced person who will certify that it is isolated and free from danger. While a tank is being built, when the walls reach a certain height (say, greater than the diameter) the

tank should be deemed to be a confined space, and the entry procedure should apply.

4. All managers and supervisors should be aware of the procedure for handover and entry to vessels.

12.3.4 Liquid Nitrogen

Supplies of liquid nitrogen should always be tested before they are off-loaded into the plant. Suppliers of liquid nitrogen often say there is no need to test, as they use different fittings on liquid nitrogen and liquid air (or oxygen) trucks and confusion is impossible. However, in several cases the impossible has happened, and liquid air (or oxygen) has been supplied instead of liquid nitrogen. One incident is described in Section 4.1 (f). Sometimes the mistake has been discovered by testing, but I know of two cases in which liquid air or oxygen was fed to a plant. Fortunately in one case a high-oxygen-concentration alarm operated and in the other case a high-temperature alarm. The first incident occurred on a plant where they always tested the regular consignments of nitrogen but did not test a special extra delivery.

If a high-temperature or high-oxygen-concentration alarm will detect a wrong delivery, is there a need to test before acceptance? The alarms are our last layer of protection; if they fail, a fire or explosion is likely, and so we should never deliberately rely on them. Our preventative measures should lie as far as possible from the top event [17].

Nitrogen boils at a lower temperature than oxygen, and so oxygen will condense on materials that are cooled with liquid nitrogen. If these materials are flammable, a fire or explosion can occur. Some pork rind that had to be ground was cooled with liquid nitrogen. When the grinder was started up, it exploded, and two men were killed.

Other hazards of liquid nitrogen and liquid air are due to their low temperature:

- Many materials become very brittle. Vehicle tires can explode, and carbon steel equipment can fail if exposed to the liquid or its vapor. A steel pressure vessel designed for use at a gauge pressure of 450 psi (30 bar) broke into 20 pieces when it was filled with cold nitrogen gas. The liquid nitrogen vaporizer should have been fitted with a low-temperature trip.

- Liquid trapped between valves will produce a large rise in pressure as it warms up.
- Spillages produce a fog, which restricts visibility [25, 26].

12.4 HEAVY OILS (INCLUDING HEAT TRANSFER OILS)

This term is used to describe oils that have a flash point above ambient temperature. They will therefore not burn or explode at ambient temperature but will do so when hot. Unfortunately many people do not realize this and treat heavy oils with a disrespect that they would never apply to gasoline, as shown by the incidents described below. Another incident was described in Section 12.2 (c). Heavy oils are widely used as fuel oils, solvents, lubricants, and heat transfer oils, as well as process materials.

12.4.1 Traces of Heavy Oil in Empty Tanks

Repairs had to be carried out to the roof of a storage tank, which had contained heavy oil. The tank was cleaned out as far as possible, and two welders started work. They saw smoke coming out of the vent and flames coming out of the hole they had cut. They started to leave, but before they could do so the tank's roof lifted, and a flame 25 m long came out. One of the men was killed and the other was badly burned. The residue in the tank continued to burn for 10–15 minutes [5].

Though the tank had been cleaned, traces of heavy oil were stuck to the sides or behind rust or trapped between plates. These traces of oil were vaporized by the welding and ignited.

Some old tanks are welded along the outside edge of the lap only, thus making a trap from which it is hard to remove liquids. Even light oils can be trapped in this way (see Section 5.4.2 (c) and Figure 5-10).

A similar incident is described in an official report [6]. A tank with a gummy deposit on the walls and roof had to be demolished. The deposit was unaffected by steaming but gave off vapor when a burner's torch was applied to the outside. The vapor exploded, killing six firemen who were on the roof at the time.

It is almost impossible to completely clean a tank (or other equipment) that has contained heavy oils, residues or polymers, or material that is solid at ambient temperature, particularly if the tank is corroded. Tanks that have contained heavy oils are more dangerous than tanks that have

contained lighter oils, such as gasoline. Gasoline can be completely removed by steaming or sweeping with nitrogen. Note also that while light oils, such as gasoline, can be detected with a combustible gas detector, heavy oils cannot be detected. Even if a heavy oil is heated above its flash point, the vapor will cool down in the detector before it reaches the sensitive element.

Before welding is allowed on tanks that have contained heavy oils, the tanks should be filled with inert gas or with fire-fighting foam generated with inert gas, *not* with fire-fighting foam generated with air (see Section 12.3.2). Filling the tank with water can reduce the volume to be inerted.

Another incident occurred when an old 45-m^3 diesel oil tank was being cut up by acetylene welding. The top half was removed, and four holes were being cut in the lower half so that it could be picked up and moved. A piece of hot slag fell onto sludge on the bottom of the tank and set it alight. The fire could not be extinguished with handheld extinguishers, and the fire department had to be called. Cold-cutting methods should be considered when equipment that cannot be cleaned has to be cut up. Other fires have been started by falling welding slag; it can fall farther than expected [28].

An unusual case of an explosion in a "vessel" containing traces of heavy oil occurred when welding was carried out on the brakes of a tractor. The heat vaporized and ignited the lubricant used in fitting the tires, and the resulting explosion killed three men.

12.4.2 Traces of Heavy Oil in Pipelines

Some old pipelines had to be demolished. They were cleaned as far as possible and then tested with a combustible gas detector. No gas or vapor was detected, so a burner was given permission to cut them up. While doing so, sitting on the pipes 4 m above the ground, a tarry substance seeped out of one of the pipes and caught fire. The fire spread to the burner's clothing, and he ended up in the hospital with burns to his face and legs. The deposit did not give off enough vapor when cold for it to have been detected by the combustible gas detector.

It is almost impossible to completely clean pipes that have contained heavy oils or polymers. When demolishing old pipelines, there should be as many open ends as possible so that pressure cannot build up. And good access should be provided so that the burner or welder can escape readily if he or she needs to do so.

12.4.3 Pools of Heavy Oil

An ore-extracting process was carried out in a building with wooden floors. But this was considered safe because the solvent used had a flash point of 42°C, and it was used cold. Leaks of solvent drained into a pit inside the building. While welding was taking place, a burning piece of rag fell into the pit, and in a few seconds the solvent film, which covered the water in the pit, was on fire. The rag acted as a wick and set fire to the solvent, although a spark or a match would not have done so. The fire spread to the wooden floor, some glass pipes burst and these added more fuel to the fire. In a few minutes the building was ablaze and two thirds of the contents were destroyed [7].

12.4.4 Spillages of Heavy Oil, Including Spillages on Insulation

The heat transfer section of a plant was filled with oil after maintenance by opening a vent at the highest point and pumping oil into the system until it overflowed out of the vent. The overflow should have been collected in a bucket, but sometimes a bucket was not used, or the bucket was overfilled. Nobody worried about small spillages because the flash point of the oil was above ambient temperature and its boiling point and auto-ignition temperature were both above 300°C.

A month after such a spillage, the oil caught fire. Some of it might have soaked into insulation, and if so, this would have caused the oil to degrade, lowering its auto-ignition temperature so that it ignited at the temperature of the hot pipework. The oil fire caused a leak of process gas, which exploded causing further localized damage and an oil fire.

All spillages, particularly those of high-boiling liquids, should be cleaned up promptly. Light oils will evaporate, but heavy oils will not. Besides the fire hazard, spillages produce a risk of slipping.

Insulation that has been impregnated with heavy oil—or any other organic liquid—should be removed as soon as possible before the oil ignites. If oil is left in contact with insulation materials, the auto-ignition temperature is lowered by 100–200°C [8] (see Section 7.3.2).

12.4.5 Heavy Oil Fireballs

Sections 9.1.1 and 12.2 describe incidents that occurred when heavy oils, at temperatures above 100°C, came into contact with water. The

water vaporized with explosive violence, and a mixture of steam and oil was blown out of the vessel, after rupturing it.

In another incident of the same nature, the oil caught fire. A furnace supplied heat transfer oil to four reboilers. One was isolated for repair and then pressure-tested. The water was drained out of the shell, but the drain valve was 8 in. above the bottom tube plate, and so a layer of water was left in the reboiler (Figure 12-2).

When the reboiler was brought back on line, the water was swept into the heat transfer oil lines and immediately vaporized. This set up a liquid hammer, which burst the surge tank. It was estimated that this required a gauge pressure of 450 psi (30 bar). The top of the vessel was blown off in one piece, and the rest of the vessel was split into 20 pieces. The hot oil formed a cloud of fine mist, which ignited immediately, forming a fireball 35 m in diameter. (Mists can explode at temperatures below the flash point of the bulk liquid; see Section 19.5.)

Recommendations that followed from this incident are:

1. Adequate facilities must be provided for draining water from heat transfer and other hot oil systems.
2. Oil rather than water should be used for pressure testing.

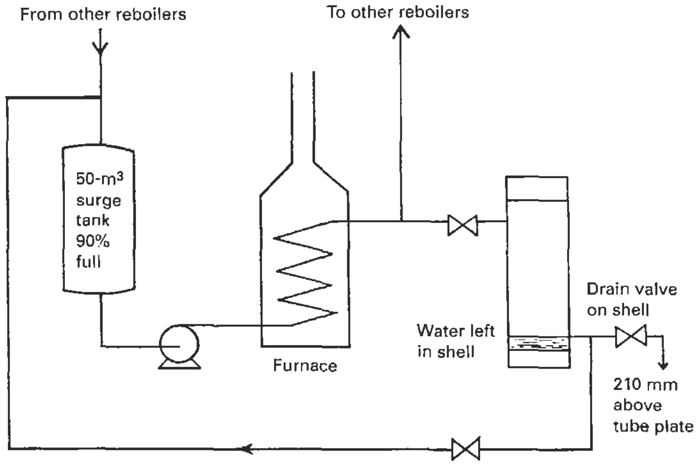


Figure 12-2. Water left in the heat exchanger was vaporized by hot oil.

3. Surge vessels should operate about half full, not 90% full as in this case.
4. In new plants, water should be considered as a heat transfer medium instead of oil. A decision to use water has to be made early in the design because the operating pressure will be higher. Although this will add to the cost, there will be savings in lower fire protection costs. In some plants the heat transfer oil is a bigger fire hazard than the process materials [9–11].

12.4.6 A Lubricating Oil Fire

An ethylene plant compressor was lubricated by a pump, which took suction from a sump. The sump was originally topped up by hand, but to save labor a pump was installed to supply oil from a storage tank some distance away. An operator forgot to shut down this pump when the sump was filled to the required level, and it was overfilled. The pump had a greater capacity than the vent on the sump, so the sump was overpressured. The pressure backed up the oil line from the gearbox, which failed. Oil spewed out and ignited. The material damage was $500,000, but the consequential loss was many times greater [18].

On chemical plants and oil refineries, steam, nitrogen, compressed air, lubricating oil, and other utility systems are responsible for a disproportionately large number of accidents. Flammable oils are recognized as a hazard, but services are given less attention. If the modification to the lubricating system had been systematically studied before it was made, as recommended in Chapter 2, a larger vent could have been installed, or a pipe-break and funnel could have been installed at the inlet to the sump.

12.4.7 Degradation of Heavy Oils

Degradation of heavy oils spilled on insulation has already been described in Sections 7.3.2 and 12.4.4. Heat transfer oils can degrade in normal use, producing both light and heavy ends. The light ends accumulate at high points and can further degrade into a mixture of carbon and rust, known as "coffee grounds," which forms hard deposits in dead-end nozzles, such as those leading to relief valves. To prevent blockages, we should vent light ends frequently and inspect relief valve nozzles whenever the relief valves are removed for routine examination.

Heavy ends can further degrade into carbon deposits on the insides of furnace tubes and lead to tube failure. Sometimes the tube blocks completely and prevents a serious spillage, but at other times spillages have produced costly and spectacular fires, as in the incident descried in Section 10.7.2 (though that one was not due to accumulation of heavy ends). To prevent tube failures, keep the concentration of heavy ends below 5% and follow the recommendations on furnace operation in Section 10.7.2 [27].

REFERENCES

1. *Safety Management* (South Africa), Apr. 1982, p. 30; and Feb. 1993, p. 36.
2. *Hazards of Air,* 6th edition, American Oil Company, Chicago, 1984.
3. *Hazards of Water,* 6th edition, American Oil Company, Chicago, 1984.
4. T. A. Kletz, "Nitrogen—Our Most Dangerous Gas," *Proceedings of the Third International Symposium on Loss Prevention and Safety Promotion in the Process Industries,* Swiss Society of Chemical Industries, 1980, p. 1518.
5. T. A. Kletz, *Journal of Hazardous Materials,* Vol. 1, No. 2, 1976, p. 165.
6. A.W.M. Davies, *Public Enquiry into a Fire at Dudgeon's Wharf on 17 July 1969,* Her Majesty's Stationery Office, London, 1970.
7. R. Hoy-Petersen, *Proceedings of the First International Symposium on Loss Prevention and Safety Promotion in the Process Industries,* Elsevier, Amsterdam, 1984, p. 325.
8. P. E. Macdermott, *Petroleum Review,* July 1976.
9. J. W. Boley, *A Guide to Effective Industrial Safety,* Gulf Publishing Co., Houston, Texas, 1977.
10. L. Pilborough, *Inspection of Chemical Plants,* Gulf Publishing Co., Houston, Texas, 1977.
11. K. Gugan, *Unconfined Vapor Cloud Explosions,* Gulf Publishing Co., Houston, Texas, 1979.
12. N. Morris, *The Chemical Engineer,* No. 437, June 1987, p. 51.
13. *Chemistry in Britain,* Vol. 22, No. 7, July 1986, p. 610.
14. *Chemical Engineering,* Dec. 2, 1977, p. 67.
15. *Bulletin,* Royal Society for the Prevention of Accidents, Birmingham, UK, May 1980.

16. *Chemical Safety Summary*, Vol. 56, No. 221, Chemical Industries Association, London, 1985, p. 4.

17. T. A. Kletz, *Learning from Accidents,* 2nd edition, Butterworth-Heinemann, Oxford, UK, 1994.

18. V. G. Geishler, *Loss Prevention,* Vol. 12, 1979, p. 10.

19. A. Jacob, *The Chemical Engineer,* No. 503, Sept. 12, 1991, p. 19.

20. Y. Guo and C. W. Kauffman, "An Experimental Investigation of Air Line Explosions Caused by Film Detonation," Paper presented at Combustion Institute Eastern Section Fall Meeting, Albany, N.Y., Oct./Nov. 1989.

21. G. R. Schoofs, *AIChE Journal,* Vol. 38, No. 9, Sept. 1992, p. 1385.

22. *Employee Suffers Oxygen Deprivation,* Safety Note No. DOE/EH-0110. U.S. Dept. of Energy, Washington, D.C., Oct. 1989.

23. *Loss Prevention Bulletin,* No. 110, Apr. 1993, p. 8.

24. *Loss Prevention Bulletin,* No. 098, Apr. 1991, p. 19.

25. *Loss Prevention Bulletin,* No. 097, Feb. 1993, p. 1.

26. British Cryogenics Council, *Cryogenics Safety Manual,* 3rd edition, Butterworth-Heinemann, Oxford, UK, 1991.

27. J. W. Bowman and R. P. Perkins, *Plant/Operations Progress,* Vol. 9, No. 1, Jan. 1990, p. 39.

28. *Occupational Health and Safety Observer,* Vol. 3, No. 12, U.S. Dept. of Energy, Washington, D.C., Dec. 1994, p. 6.

Chapter 13

Tank Trucks and Cars

This chapter is not concerned with accidents on the road. Rather, it describes some of the many incidents that have occurred while tank trucks and cars (known in Europe as road and rail tankers) were being filled or emptied. Section 18.8 shows how hazard and operability studies have been used to spot potential hazards in filling systems, and Section 22.3 describes some runaway reactions in tank trucks and cars..

13.1 OVERFILLING

Tank trucks and cars have been overfilled on many occasions, both when filled automatically and when filled by hand.

In automatic systems the filler sets the quantity to be filled on a meter, which closes a valve when this required quantity has been delivered. Overfilling has occurred because the wrong quantity was set on the meter, because there was already some liquid in the tank (left over from the previous load), and because the filling equipment failed. For these reasons many companies now fit their tank trucks with high-level trips, which automatically close a valve in the filling line [8].

Tank trucks and cars that are filled by hand have been overfilled because the filler left the job for a few minutes and returned too late. On one occasion an operator thought a tank truck had a single-compartment tank when in fact there were two compartments. He tried to put the full load into one compartment.

On another occasion, after a tank truck had been filled during the night, the operator completed a filling certificate—a very small piece of paper—and slipped it inside the dispatch papers. This was the usual prac-

tice. When the next shift came on duty, the driver had not returned to get the truck. The overnight record sheets had all been sent to the plant office. So the operator shook the dispatch papers to see if there was a filling certificate among them. Nothing fell out because the certificate was caught up in the other papers. The operator therefore started to fill the tanker again.

In contrast, a case of overfilling, which was the subject of an official report [1], was due to the poor design of complex automatic equipment at a large terminal for loading gasoline and other hydrocarbons.

The grade and quantity of product required were set on a meter. The driver inserted an authorization card and pressed the Start button. The required quantity was then delivered automatically. The filling arm had to be lowered before filling could start.

One day the automatic equipment broke down, and the foreman decided to change over to manual filling. He asked the drivers to check that the hand valves on the filling lines were shut, but he did not check himself. He then operated the switches that opened the automatic valves. *Some of the hand valves were open.* Gasoline and other products came out, overfilled the tanker (or splashed directly on the ground) and caught fire. Three men were killed, 11 injured, and the whole row of 18 filling points was destroyed.

To quote from the official report, "The decision to override the individual controls on the loading arms by means of a central switchboard, without the most rigid safeguards, was a tragic one. After its installation an accident from that moment on became inevitable sooner or later.

"That this switchboard was installed, with the approval of the terminal management . . . in a switchroom from which the loading stands were not visible, suggests some failure to take into account the basic fundamentals of safety in operation of plant.

". . . had the same imagination and the same zeal been displayed in matters of safety as was applied to sophistication of equipment and efficient utilization of plant and men, the accident need not have occurred."

13.2 BURST HOSES

Hoses have failed while tank trucks or cars were being filled or emptied for all the reasons listed in Section 7.1.6, in particular because damaged hoses or hoses made from the wrong material were used. However,

the most common cause of hose failure is the tanker driving away before the hose is disconnected.

The following incidents are typical:

(a) A tank truck was left at a plant for filling with liquefied flammable gas. Some hours later, the transport foreman assumed that it would be ready and sent a driver to get it. There was no one in the plant office, so the driver went to the loading bay. He found that the truck was grounded and that the grounding lead had been looped through the steering wheel—the usual practice—to prevent the driver from driving away before disconnecting it. He removed the lead and drove off, snapping off the filling branch and tearing the hose that was connected to the vent line. Fortunately, there was no flow through the filling line at the time though the valves were open, and the spillage was relatively small. It did not catch fire.

Plant instructions stated that a portable barrier should be put in front of tank trucks being filled, but the barrier was not being used. However, if it had been in use, the driver might have removed it.

A device that can be fitted to a tank truck to prevent anyone from driving it away while a hose is connected is described in Reference 2. A plate is fixed in front of the hose connection. To connect the hose, this plate has to be moved aside, and this applies the brakes. Reference 3 describes a special type of hose that seals automatically if it breaks; there are also other types.

Remotely operated emergency isolation valves (see Section 7.2.1) should be fitted on filling lines. If the hose breaks for any reason, the flow can be stopped by pressing a button located at a safe distance. Reverse flow from the tank truck or car can be prevented by a check valve.

Note that it is not necessary to ground tank trucks containing liquefied flammable gases because no air is present in the tank.

(b) Gasoline was being discharged at a service station from a tank truck, which was carrying diesel fuel in one compartment. To save time the driver decided to discharge the diesel fuel while discharging the gasoline. To do this he had to move the tank truck about 1–2 m.

He drove the truck slowly forward, while the discharge of fuel continued. The hose caught on an obstruction and was pulled part

way out of its fastening. Gasoline escaped and caught fire. The service station and tank truck were destroyed [4].

(c) Similar incidents have occurred at gasoline filing stations when motorists have driven off before removing the filling nozzles from their cars. In one case, the pump and nozzle were damaged and sparking ignited the spilled gasoline.

13.3 FIRES AND EXPLOSIONS

A number of explosions or fires have occurred in tank trucks or cars while they were being filled. The most common cause is "switch filling." A tank contains some flammable vapor, such as gasoline vapor, from a previous load and is then filled with a safer, higher-boiling liquid, such as gas oil. The gas oil is not flammable at ambient temperature. So no special precautions are normally necessary to prevent the formation of static electricity. The tank may be filled quickly—may even be splash-filled—a static charge is formed, and a spark jumps from the liquid to the wall of the tank, igniting the gasoline vapor.

A similar incident occurred in a tank truck used to carry waste liquids. While it was being filled with a nonflammable liquid and the driver was standing on the top, smoking, an explosion occurred, and the manhole cover was thrown 60 m. On its previous journey the tank truck had carried a waste liquid containing dissolved flammable gas. Some of the gas was left in the tank and was pushed out when it was filled with the next load. For other examples see Reference 10.

Flammable liquids should never be splash-filled, even though they are below their flash points. The splash filling may form a mist, which can be ignited by a static discharge. Mists, like dusts, can be ignited at any temperature (see Section 19.5).

On one occasion a tank truck was being splash-filled with gas oil, flash point 60°C. The splashing produced a lot of mist, and it also produced a charge of static electricity on the gas oil. This discharged, igniting the mist. There was a fire with flames 10 m high but no explosion. The flames went out as soon as the mist had been burned.

Many thousands of tank trucks had been splash-filled with gas oil at this installation before conditions were exactly right for a fire to occur. When handling flammable gases or liquids, we should never say, "It's OK. We've been doing it this way for 20 years and have never had a

fire." Such a statement should be made only if an explosion in the 21st year is acceptable.

Note that grounding a tank truck will not prevent ignition of vapor by a discharge of static electricity. Grounding will prevent a discharge from the tank to earth, but it will not prevent a discharge from the liquid in the tank to the tank or to the filling arm.

There is more information on static electricity in Chapter 15.

13.4 LIQUEFIED FLAMMABLE GASES

Tank trucks or cars that carry liquefied gases under pressure at ambient temperature present additional hazards.

When the tanks are filled, the vapor is vented to a stack or back to the plant through a vapor return line, which is fitted to the top of the tank. An official report [5] described a fire that occurred because the fillers had not bothered to connect up this vapor return line. Vapors were discharged into the working area. Seven people were injured.

Following this incident, a survey at another large installation showed that the fillers there were also forgetting to connect up the vapor lines. Reference 5 also reports that at another plant the vapor return line was connected in error to another filling line. The vapor could not escape, the pressure in the tank rose, and the filling hose burst. There was no emergency isolation valve in the filling line, no check valve on the tank (see Section 13.2 a), and no excess flow valve on either, so the spillage was substantial.

Vapor return lines and filling lines should be fitted with different sizes or types of connections.

13.5 COMPRESSED AIR

Compressed air is often used to empty tank trucks and cars. Plastic pellets are often blown out of tank trucks. When the tank is empty, the driver vents the tank and then looks through the manhole to check that the tank is empty. One day a driver who was not regularly employed on this job started to open the manhole before releasing the pressure. When he had opened two out of five quick-release fastenings, the manhole blew open. The driver was blown off the tank top and killed.

Either the driver forgot to vent the tank or thought it would be safe to let the pressure (a gauge pressure of 10 psi or 0.7 bar) blow off through the manhole. After the accident the manhole covers were replaced by a

different type in which two movements are needed to release the fastenings. The first movement allows the cover to be raised about ¼ in. while still capable of carrying the full pressure. If the pressure has not been blown off, this is immediately apparent, and the cover can be resealed or the pressure allowed to blow off.

In addition, the vent valve was repositioned at the foot of the ladder [6].

Many of those concerned were surprised that a pressure of "only ten pounds" could cause a man to be blown off the top of the tank. They forgot that 10 psi is not a small pressure. It is 10 lbs of force on every square inch (see Section 12.1).

A similar incident is described in Section 17.1.

13.6 TIPPING UP

On several occasions tank trailers have tipped up because the rear compartments were emptied first, as shown in Figure 13-1.

It is not always possible to keep the trailer connected to the truck's unit during loading/unloading. If it is not connected, the front compartments should be filled last and emptied first or a support put under the front of the trailer.

Figure 13-1. A tank trailer may tip up if the rear compartments are emptied first.

Some tank trailers are fitted with folding legs. Some designs are difficult to lubricate adequately and difficult to maintain, and as a result, a number have collapsed.

13.7 EMPTYING INTO OR FILLING FROM THE WRONG PLACE

On many occasions tank trucks have been discharged into the wrong tank. The following incident is typical of many.

A tank truck containing isopropanol arrived at a plant during the night. It was directed to a unit that received regular supplies by tank trucks. The unit was expecting a load of ethylene glycol. So without looking at the label or the delivery note, unit staff members emptied the tank truck into the ethylene glycol tank and contaminated 100 tons of ethylene glycol.

Fortunately in this case the two materials did not react. People who have emptied acid into alkali tanks have been less fortunate. A plant received caustic soda in tank cars and acid in tank trucks. One day a load of caustic soda arrived in a tank truck. It was labeled Caustic Soda, the delivery papers said it was caustic soda, and the hose connections were unusual. But the operators had a mind-set (see Section 3.3.5) that anything in a tank truck was acid, and they spent two hours making an adaptor to enable them to pump the contents of the tank truck into the acid tank.

A plant received tetra-ethyl lead (TEL) and hydrogen fluoride (HF) in tank cars of different shapes, colors, and markings. One day a load of HF arrived in a tank car of the type normally used for TEL. It was therefore put into the siding alongside the TEL off-loading point, and an operator started to transfer the contents into the TEL tank. He stopped when he noticed white fumes coming out of the vent on the tank car. The contents of the TEL tank were ruined, but fortunately the reaction did not run away [9]. It is difficult not to sympathize with the operators. The delivery of HF in a tank car of the type used for TEL set a trap for them (see Chapter 3). The supplier might reasonably have been expected to draw attention to the change.

On other occasions tank trucks have been filled with the wrong material. In particular, liquid oxygen or liquid air has been supplied instead of liquid nitrogen. One incident, the result of confusion over labeling, was described in Section 4.1 (f).

I do not know of any case in which delivery of liquid oxygen instead of liquid nitrogen caused an explosion. But, as stated in Section 12.3.1, in one case the "nitrogen" was used to inert a catalyst bed, and the catalyst got hot; in another case a high-oxygen-concentration alarm in the plant sounded, and in several cases check analyses showed that oxygen had been supplied.

Many suppliers of liquefied gases state that they use different hose connections for liquid oxygen and liquid nitrogen so mistakes cannot arise. However, mistakes *have* occurred, possibly because of the well-known tendency of operators to acquire adaptors.

Liquid nitrogen should always be analyzed before it is off-loaded. The same applies in other cases where delivery of the wrong material could have serious unwanted results, such as a fire or runaway reaction, as in the two incidents that follow. If analysis causes too much delay, the new load should be put in a holding tank.

- After a load of diesel fuel intended for stand-by generators had been off-loaded into the stock tank, it was found to contain too much particulate matter. This could have affected the performance of the generators [11].
- As the result of a mix-up at a distribution center, two tank truck drivers received each other's papers. One of the trucks carried a load of sodium chlorite solution, and the other carried epichlorohydrin. The chlorite truck went to the customer who was expecting epichlorohydrin and was off-loaded into a tank that already contained some epichlorohydrin. The result was an explosion and a serious fire; fumes and smoke led to the closure of the bridges over the Severn Estuary, UK [12, 13].

Suppliers' papers tell us what they intend to deliver, not what is in the tank truck or car. We can find that out either by analyzing the contents or by seeing what happens.

The following incident involved cylinders rather than bulk loads, but it shows how alertness to an unusual observation can prevent an accident.

A plant used nitrogen in large cylinders. One day a cylinder of oxygen, intended for another plant, was delivered in error. The foreman noticed that the cylinder had an unusual color and unusual fittings, and he thought it strange that only one was delivered. Usually several cylinders

were delivered at a time. Nevertheless he accepted the cylinder. He did not notice that the invoice said Oxygen.

The invoice was sent as usual to the purchasing department for payment. The young clerk who dealt with it realized that oxygen had been delivered to a unit that had never received it before. She told her supervisor, who telephoned the plant, and the error came to light.

For another success story, see Section 11.7.

13.8 CONTACT WITH LIVE POWER LINES

The manhole covers on tank cars are sometimes sealed with wires. Loose ends of wires protruding above the manhole cover have come into contact with the overhead electric wire, which supplies power to the train, and caused a short circuit.

In the UK there is normally a gap of 4 in. between the highest point of the tank car and the lowest point of the cables, but if the gap falls below 2 in. arcing may occur [7].

Somewhat similar incidents have occurred on railway lines powered by a third electrified rail. The cap covering the discharge pipe has vibrated loose, the retaining chain has been too long, and the cap has contacted the third rail [7].

REFERENCES

1. H. K. Black, *Report on a Fatal Accident and Fire at the West London Terminal on 1 April 1967,* Her Majesty's Stationery Office, London, 1967.
2. T. A. Kletz, *Loss Prevention,* Vol. 10, 1976, p. 151.
3. *Petroleum Review,* July 1976, p. 433.
4. *Petroleum Review,* July 1976, p. 428.
5. *Annual Report of H. M. Inspectors of Explosives for 1967,* Her Majesty's Stationery Office, London, 1968.
6. T. A. Kletz, *Lessons from Disaster: How Organizations Have No Memory and Accidents Recur,* co-published by Institution of Chemical Engineers, Rugby, UK, and Gulf Publishing Co., Houston, Texas, 1993, Chapter 2.
7. *Petroleum Review,* Apr. 1976, p. 241.

8. J. N. Baker, *Measurement and Control,* Vol. 18, Apr. 1985, p. 104.
9. *Petroleum Review,* June 1985, p. 36.
10. T. H. Pratt, *Process Safety Progress,* Vol. 15, No. 3, Fall 1996, p. 177.
11. *Operating Experience Weekly Summary,* No. 97-06, Office of Nuclear and Safety Facility, U.S. Dept. Of Energy, Washington, D.C., 1997, p. 3.
12. *The Chemical Engineer,* No. 620, Oct. 10, 1996, p. 10; and No. 621, Oct. 24, 1996, p. 7.
13. *The Industrial Emergency Journal,* Vol. 1, No. 2, Oct./Nov. 1996, p. 14.

Chapter 14

Testing of Trips and Other Protective Systems

The driver of a ramshackle Maputo taxi that had holes in the floor and kept breaking down was asked if all the gears worked. "Yes," he said, "but not all at the same time."

—*Daily Telegraph* (London), Jan. 7, 1995

Many accidents have occurred because instrument readings or alarms were ignored (see Sections 3.2.8, 3.3.1, and 3.3.2). Many other accidents, including Bhopal (see Section 21.1), have occurred because alarms and trips were not tested or not tested thoroughly, or because alarms and trips were made inoperative or their settings altered, both without authority. These and some related accidents are described below.

Microprocessor-based control systems are being increasingly used in place of traditional instrumentation. Some accidents that have occurred on these systems are described in Chapter 20.

14.1 TESTING SHOULD BE THOROUGH

All protective equipment should be tested regularly, or it may not work when required. While it is sufficient to test relief valves every year or every two years, instrumented alarms and trips are less reliable and should be inspected every month or so.

Testing must be thorough and as near as possible to real-life situations, as shown by the following incidents:

(a) A high-temperature trip on a furnace failed to operate. The furnace was seriously damaged. The trip did not operate because the pointer touched the plastic front of the instrument case, and this prevented it from moving to the trip level. The instrument had been tested regularly—by injecting a current from a potentiometer—but to do this *the instrument was removed from its case and taken to the workshop.*

(b) A reactor was fitted with a high-temperature trip, which closed a valve in the feed line. When a high temperature occurred, the trip valve failed to close although it had been tested regularly.

Investigation showed that the pressure drop through the trip valve—a globe valve—was so high that the valve could not close against it. There was a flow control valve in series with the trip valve (Figure 14-1), and the trip normally closed this valve as well. However, this valve failed in the open position—this was the reason for the high temperature in the reactor—and the full upstream pressure was applied to the trip valve.

Emergency valves should be tested against the maximum pressure or flow they may experience and, whenever possible, should be installed so that the flow assists closing.

(c) If the response time of protective equipment is important, it should always be measured during testing. For example, machinery is often interlocked with guards so that if the guard is opened, the machinery stops. Brakes are often fitted so that the machinery stops quickly. The actual stopping time should be measured at regular intervals and compared with the design target.

Another example: a mixture of a solid and water had to be heated to 300°C at a gauge pressure of 1,000 psig (70 bar) before the

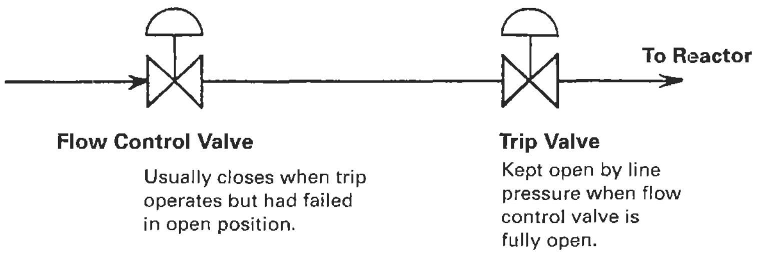


Figure 14-1. When the control valve was open, the pressure prevented the trip valve from closing.

solid would dissolve. The mixture was passed through the tubes of a heat exchanger while hot oil, at low pressure, was passed over the outside of the tubes. It was realized that if a tube burst, the water would come into direct contact with the hot oil and would turn to steam with explosive violence. An automatic system was therefore designed to measure any rise in the oil pressure and to close four valves, in the water and oil inlet and exit lines. The heat exchanger was also fitted with a rupture disc, which discharged into a catchpot. The system was tested regularly, but nevertheless, when a tube actually burst most of the oil was blown out of the system and caught fire, as the valves had taken too long to close. They had been designed to close quickly but had gotten sluggish; the time of response was not measured during the test, so no one knew that they were not responding quickly enough.

Procedures, like equipment, also take time to operate. For example, how long does it take to empty your building when the fire alarm sounds? Is this quick enough?

(d) A large factory could be supplied with emerency power from a diesel-driven generator. It was tested regularly to ensure that the diesel engine started up when required. When the power supply actually failed, the diesel generator started up, but the relay that connected it to the distribution system failed to operate.

The emergency supply was tested when the distribution system was live. No one understood how the emergency circuits worked and did not realize that they were not being thoroughly tested [2].

(e) An example from another industry: for many years railway carriage doors in the United Kingdom opened unexpectedly from time to time, and passengers fell out. Afterward the locks were removed from the doors and sent for examination. No faults were found, and it was concluded that passengers had opened the doors. However, it was not the locks that were faulty but the alignment between the locks and the recesses in the doors. This was faulty and allowed them to open [3].

(f) A plant was pressure-tested before startup, but the check valves (nonreturn valves, NRV) in the feed lines to each unit (Figure 14-2) made it impossible to test the equipment to the left of them. A leak of liquefied petroleum gas (LPG) occurred during startup at the

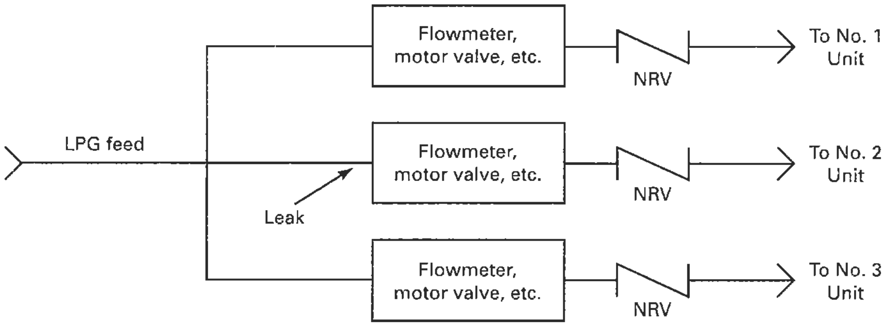


Figure 14-2. The check valves (nonreturn valves NRV) prevented a leak test of the equipment to the left of them. During startup a leak occurred at the point indicated.

point indicated. The three check valves were then replaced by a single one in the common feed line at the extreme left of the diagram.

(g) Before testing an interlock or isolation to make sure it is effective, ask what will happen if it is not. For example, if a pump or other item of equipment has been electrically isolated by removing the fuses, it should be switched on to check that the correct fuses have been withdrawn. Suppose they have not; will the pump be damaged by starting it dry?

A radioactive source was transferred from one container to another by remote operation in a shielded cell. A radiation detector, interlocked with the cell door, prevented anyone from opening the cell door when radiation could be detected inside it. To make sure the interlock was working, an operator tried to open the cell door, by remote control, during a transfer. He found he could open it. He then found that the closing mechanism would not work. Fortunately he had not opened the door very far.

(h) Do not test a trip or interlock by altering the set-point. The trip or interlock may operate at the altered set-point, but that does not prove it will operate at the original set-point.

14.2 ALL PROTECTIVE EQUIPMENT SHOULD BE TESTED

This section lists some protective equipment that has often been overlooked and not included in testing schedules.

14.2.1 Leased Equipment

After a low-temperature trip on a nitrogen vaporizer failed to operate, it was found that the trip was never tested. The equipment was rented, and the user assumed—wrongly—that the owner would test it.

14.2.2 Emergency Valves

A pump leaked and caught fire. It was impossible to reach the suction and delivery valves. But there was a second valve in the suction line between the pump and the tank from which it was taking suction, situated in the tank dike. Unfortunately this valve was rarely used and was too stiff to operate.

All valves—whether manual or automatic—that may have to be operated in an emergency should be tested regularly (weekly or monthly). If completely closing a valve will upset production, it should be closed halfway during testing and closed fully during shutdowns.

Emergency blowdown valves are among those that should be tested regularly. Reference 5 describes in detail the measures necessary to test emergency isolation valves when very high reliability is needed.

14.2.3 Steam Tracing

A furnace feed pump tripped out. The flowmeter was frozen, so the low-flow trip did not operate. Two tubes burst, causing a long and fierce fire. The structure and the other tubes were damaged, and the stack collapsed.

In cold weather, the trace heating on instruments that form part of trip and alarm systems should be inspected regularly. This can be part of the test routine, but more frequent testing may be necessary.

14.2.4 Relief Valves, Vents, Flame Arrestors, Etc.

Section 10.4.2 lists some items that should be registered for inspection as part of the relief valve register. Section 2.2 (a) described an accident that killed two men. A vent was choked, and the end of the vessel was blown off by compressed air.

Open vents, especially those on storage tanks, are often fitted with flame arrestors. If the vents, and in particular the flame arrestors, are not

kept clean, they are liable to choke, and the tanks maybe sucked in (see Section 5.3 a). If the flame arrestors are ineffective, a lightning strike or other external source of ignition may ignite the flammable mixture often present inside the tank, above the liquid level, and produce an explosion. According to a 1989 report, in the Province of Alberta, Canada, alone, failures of flame arrestors were responsible for 10–20 tank explosions every year. Some of the failures were due to damage not detected during inspection, others to unsuitable design [4].

14.2.5 Other Equipment

Other equipment, in addition to that already mentioned, that should be tested regularly includes the following:

- Check valves and other reverse-flow prevention devices, if their failure can affect the safety of the plant.
- Drain holes in relief valve tailpipes. If they choke, rainwater will accumulate in the tailpipe (see Section 10.4).
- Drain valves in tank dikes. If they are left open, the dike is useless.
- Emergency equipment, such as diesel-driven fire water pumps and generators.
- Filters for both gases and liquids, including air filters. Their performance should be checked.
- Fire and smoke detectors and fire-fighting equipment.
- Grounding connections, especially the movable ones used for grounding trucks.
- Labels (see Chapter 4) are a sort of protective equipment. They vanish with remarkable speed, and regular checks should be made to make sure they are still there.
- Mechanical protective equipment, such as overspeed trips.
- Nitrogen blanketing (on tanks, stacks, and centrifuges).
- Passive protective equipment, such as insulation. If 10% of the fire insulation on a vessel is missing, the rest is useless.
- Spare pumps, especially those fitted with auto-starts.
- Steam traps.
- Trace heating (steam or electrical).

- Trips, interlocks, and alarms.
- Valves, remotely operated and hand-operated, that have to be used in an emergency.
- Ventilation equipment (see Section 17.6).
- Water sprays and steam curtains.

Finally, equipment used for carrying out tests should itself be tested.

If equipment is not worth testing, then you don't need it.

Trips and interlocks should be tested after a major shutdown, especially if any work has been done on them. The following incidents demonstrate the need to test all protective equipment:

(a) A compressor was started up with the barring gear engaged. The barring gear was damaged.

The compressor was fitted with a protective system that should have made it impossible to start the machine with the barring gear engaged. But the protective system was out of order. It was not tested regularly.

(b) In an automatic fire-fighting system, a small explosive charge cut a rupture disc and released the fire-fighting agent, halon. The manufacturers said it was not necessary to test the system. To do so, a charge of halon, which is expensive, would have to be discharged.

The client insisted on a test. The smoke detectors worked, and the explosive charge operated, but the cutter did not cut the rupture disc. The explosive charge could not develop enough pressure because the volume between it and the rupture disc was too great. The volume had been increased as the result of a change in design: installation of a device for discharging the halon manually.

(c) A glove box on a unit that handled radioactive materials was supposed to be blanketed with nitrogen, as some of the materials handled were combustible. While preparing to carry out a new operation, an operator discovered that the nitrogen supply was disconnected and that there was no oxygen monitor. The supply was disconnected several years before when nitrogen was no longer needed for process use, and the fact that it was still needed for blanketing was overlooked. Disconnecting a service was not seen as a modification and was not treated as such. The oxygen analyzer had apparently never been fitted [6].

One sometimes comes across a piece of protective equipment that is impossible to test. All protective equipment should be designed so that it can be tested easily.

14.3 TESTING CAN BE OVERDONE

An explosion occurred in a vapor-phase hydrocarbon oxidation plant, injuring ten people and seriously damaging the plant, despite the fact that it was fitted with a protective system that measured the oxygen content and isolated the oxygen supply if the concentration approached the flammable limit.

It is usual to install several oxygen analyzers, but this plant was fitted with only one. The management therefore decided to make up for the deficiency in numbers by testing it daily instead of weekly or monthly.

The test took more than an hour. The protective system was therefore out of action for about 5% of the time. There was a chance of 1 in 20 that it would not prevent an explosion because it was being tested. It was, in fact, under test when the oxygen content rose.

14.4 PROTECTIVE SYSTEMS SHOULD NOT RESET THEMSELVES

(a) A gas leak occurred at a plant and caught fire. The operator saw the fire through the window of the control room and operated a switch, which should have isolated the feed and opened a blowdown valve. Nothing happened. He operated the switch several times, but still nothing happened. He then went outside and closed the feed valve and opened the blowdown valve by hand.

The switch operated a solenoid valve, which vented the compressed air line leading to valves in the feed and blowdown lines (Figure 14-3). The feed valve then closed, and the blowdown valve opened. This did not happen instantly because it took a minute or so for the air pressure to fall in the relatively long lines between the solenoid valve and the other valves.

The operator expected the system to function as soon as he operated the switch. When it did not, he assumed it was faulty. Unfortunately, after operating the switch several times, he left it in its normal position.

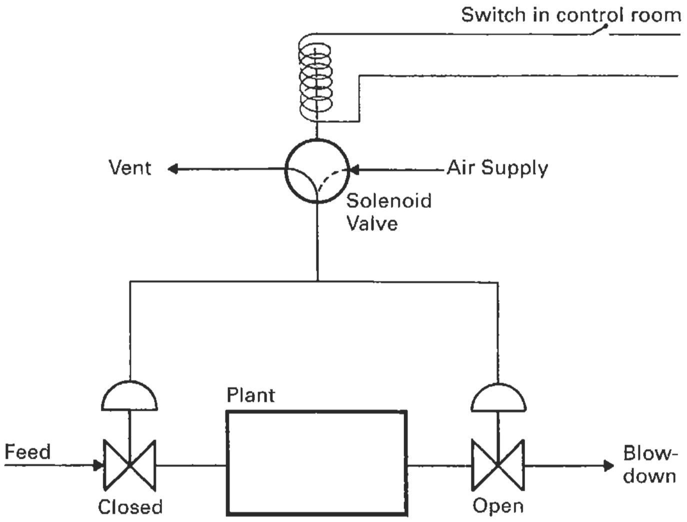


Figure 14-3. An automatic system, which will take a minute or so to operate.

The operator had tested the system on several occasions, as it was used at every shutdown. However, it was tested in conditions of no stress, and he did not notice that it took a minute or so to operate. The solenoid valve should have been fitted with a latch so that once the switch had been operated, the solenoid valve could not return to its normal position until it was reset by hand.

(b) A liquid-phase hydrocarbon oxidation plant was fitted with a high-temperature trip, which shut off the air and opened a drain valve that dumped the contents of the reactor in a safe place (Figure 14-4). If the air valve reopened after a dump, a flammable mixture could form in the reactor.

One day the temperature-measuring device gave a false indication of high temperature. The air valve closed, and the drain valve opened. The temperature indication fell, perhaps because the reactor was now empty. The drain valve stayed open, but the air valve reopened, and a flammable mixture was formed in the reactor. Fortunately it did not ignite.

The air valve reopened because the solenoid valve in the instrument air line leading to the air valve would not stay in the tripped position. It should have been fitted with a latch.

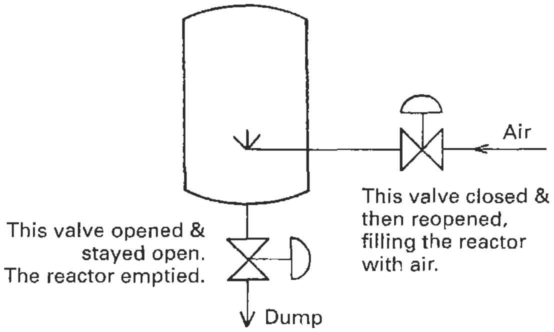


Figure 14-4. When the air valve reopened after a dump, a flammable mixture formed in the reactor.

14.5 TRIPS SHOULD NOT BE DISARMED WITHOUT AUTHORIZATION

Many accidents have occurred because operators made trips inoperative (that is, disarmed, blocked, or deactivated). The following incidents are typical:

(a) Experience shows that when autoclaves or other batch reactors are fitted with drain valves, the valves may be opened at the wrong time and the contents tipped onto the floor, often inside a building. To prevent this, the drain valves on a set of reactors were fitted with interlocks so that they could not be opened when the pressure was above a preset value. Nevertheless, a drain valve was opened when a reactor was up to pressure, and a batch emptied onto the floor. The inquiry disclosed that the pressure-measuring instruments were not very reliable. So the operators had developed the practice of defeating the interlocks either by altering the indicated pressure with the zero adjustment screw or by isolating the instrument air supply.

One day the inevitable happened. Having defeated the interlock, an operator opened a drain valve in error instead of a transfer valve.

Protective equipment may have to be defeated from time to time, but this should only be done after authorization in writing by a responsible person. And the fact that the equipment is out of action should be clearly signaled—for example, by a light on the panel.

(b) Soon after a startup, part of a unit was found to be too hot. Flanged joints were fuming. It was then found that the combined temperature controller and high-temperature trip had been unplugged from the power supply.

Trips should normally be designed so that they operate if the power supply is lost. If this will cause a dangerous upset in plant operation, then an alarm should sound when power is lost. Trips should be tested at startup if they have been worked on during a shutdown. Particularly important trips, such as those on furnaces and compressors and high-oxygen concentration trips, should always be tested after a major shutdown.

The most common cause of a high temperature (or pressure, flow, level, etc.) is a fault in the temperature measuring or control system.

(c) Trips and interlocks may have to be disarmed (that is, made inoperative) so that equipment can be maintained. The operators or maintenance workers may then forget to re-arm the trip or interlock. For example, to maintain an emergency diesel generator, the auto-start mechanism was blocked. According to the procedure, when work is complete, one electrician should remove the block, and another should verify that it has been removed. Both signed the procedure to indicate that the block was removed. Nevertheless, a week later a routine test found that the block was still in position [7].

As stated in Sections 1.2.7 (e) and 3.2.7 (b), checking procedures often break down, as the first person assumes the checker will spot anything missed; after a while the checker, having never found anything wrong, stops checking. When safety equipment has to be blocked or disarmed, this should be clearly signaled by a light or prominent notice on the panel.

(d) On computer-controlled plants, it may be possible to override an interlock by means of a software block. On one plant passwords and codes were needed for access to the program. They were kept under lock and key and issued only to electricians and engineering staff, but nevertheless 40 people had access to them. When an interlock was found, by routine tests, to be blocked, all 40 denied any knowledge. A secret shared by 40 people is no secret.

(e) At Gatwick airport, UK, an employee put his head through the hatch in the driver's cab of a cargo transfer vehicle. He thought the vehicle had stopped, but it was still moving slowly, and he became trapped between the vehicle and a nearby pillar. Fortunately he was only bruised. An interlock, which should have stopped the vehicle when the hatch was opened, had been taped over to improve the ventilation of the cab. According to the report, the company should have checked the safety equipment regularly, and a systematic assessment of the operation could have identified the risk. The company was fined [8].

(f) Alarms were deactivated, by reprogramming a data logger, to prevent them from sounding during the routine monthly test of an emergency generator. Afterward those involved forgot to reactivate the alarms. This was not discovered until nine days later, when someone looked at the data logger print-out and noticed the alarms were still listed as deactivated. There were no written logs, policies, or procedures for deactivating the alarms.

    In another similar case, the deactivation was noted in the plant log book, but few people look at old logs. The deactivation was discovered during an upset, when someone realized that an alarm had not sounded. As stated in (c) above, if an alarm is temporarily out of action, this should be prominently signaled [9].

(g) If disarming an interlock is occasionally necessary, the procedure for doing so should not be too easy, as the railways discovered long ago. Interlocks prevent a signal from being set at Go if another train is already in the section of track that it protects. An interlock occasionally has to be bypassed, for example, when a train has broken down or when the equipment for detecting the presence of a train has failed. Originally a single movement of a key was all that was necessary, and this caused several accidents. A change was then made. To get the key, the signalman (dispatcher) had to break a glass and then send for a technician to repair it. Everyone knew he had used the key, and he was less ready to use it. In an alternative system, a handle had to be turned 100 times. This gave ample time for him to consider the wisdom of his action [10].

Many of these incidents show the value of routine testing.

14.6 INSTRUMENTS SHOULD MEASURE DIRECTLY WHAT WE NEED TO KNOW

An ethylene oxide plant tripped, and a light on the panel told the operator that the oxygen valve had closed. Because the plant was going to be restarted immediately, he did not close the hand-operated isolation valve as well. Before the plant could be restarted, an explosion occurred. The oxygen valve had not closed, and oxygen continued to enter the plant (Figure 14-5).

The oxygen valve was closed by venting the air supply to the valve diaphragm, by means of a solenoid valve. The light on the panel merely said that the solenoid had been de-energized. Even though the solenoid is de-energized, the oxygen flow could have continued because:

1. The solenoid valve did not open.
2. The air was not vented.
3. The trip valve did not close.

Actually the air was not vented. The 1-in. vent line on the air supply was choked by a wasp nest. Whenever possible we should measure directly what we need to know and not some other parameter from which it can be inferred [1].

Other incidents in which operators relied on automatic valves and did not back them up with hand valves are described in Sections 17.3 (b) and 17.5 (c).

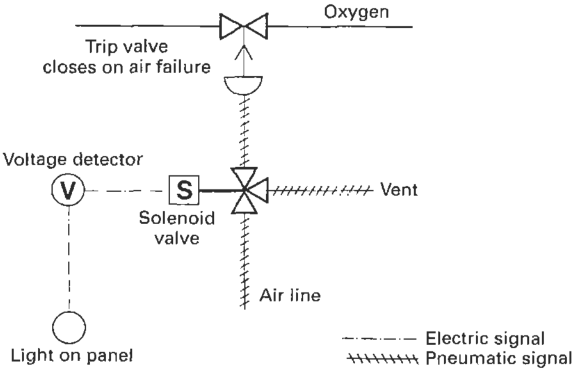


Figure 14-5. The light shows that the solenoid is de-energized, not that the oxygen flow has stopped.

14.7 TRIPS ARE FOR EMERGENCIES, NOT FOR ROUTINE USE

(a) Section 5.1.1 described how a small tank was filled every day with sufficient raw material to last until the following day. The operator watched the level in the tank and switched off the filling pump when the tank was 90% full. This system worked satisfactorily for several years before the inevitable happened and the operator allowed the tank to overfill. A high-level trip was then installed to switch off the pump automatically if the level exceeded 90%. To everyone's surprise the tank overflowed again after about a year.

When the trip was installed it was assumed that:

1. The operator will occasionally forget to switch off the pump in time, and the trip will then operate.
2. The trip will fail occasionally (about once in two years).
3. The chance that both will occur at the same time is negligible.

However, it did not work out like this. The operator decided to rely on the trip and stopped watching the level. The manager and foreman knew this but were pleased that the operator's time was being utilized better. A simple trip fails about once every two years so the tank was bound to overflow after a year or two. The trip was being used as a process controller and not as an emergency instrument.

After the second spillage the following options were considered:

1. Persuade the operator to continue to watch the level. This was considered impracticable if the trip was installed.
2. Remove the trip, rely on the operator, and accept an occasional spillage.
3. Install two trips, one to act as a process controller and the other to take over if the first one fails.

(b) When a furnace fitted with a low-flow trip has to be shut down, it is common practice to stop the flow and let the low-flow trip isolate the fuel supply to the burners. In this way the trip is tested without upsetting production.

On one occasion the trip failed to operate, and the furnace coils were overheated. The operator was busy elsewhere on the unit and was not watching the furnace.

All trips fail occasionally. So if we are deliberately going to wait for a trip to operate, we should watch the readings and leave ourselves time to intervene if the trip fails to work.

14.8 TESTS MAY FIND FAULTS

Whenever we carry out a test, we may find a fault, and we must be prepared for one.

After changing a chlorine cylinder, two workers opened the valves to make sure there were no leaks on the connecting pipework. They did not expect to find any, so they did not wear air masks. Unfortunately there were some small leaks, and they were affected by the chlorine.

The workers' actions were not very logical. If they were sure there were no leaks, there was no need to test. If there was a need to test, then leaks were possible, and air masks should have been worn.

Similarly, pressure tests (at pressures above design, as distinct from leak tests at design pressure) are intended to detect defects. Defects may be present—if we were sure there were no defects, we would not need to pressure-test—and therefore we must take suitable precautions. No one should be in a position where he or she may be injured if the vessel or pipework fails (see Section 19.2).

14.9 SOME MISCELLANEOUS INCIDENTS

(a) A radioactive-level indicator on the base of a distillation column was indicating a low level although there was no doubt that the level was normal. Radiography of pipewelds was in operation 60 m away, and the radiation source was pointing in the direction of the radiation detector on the column. When the level in the column is high the liquid absorbs radiation; when the level is low more radiation falls on the detector. The detector could not distinguish between radiation from the normal source and radiation from the radiographic source and registered a low level.

(b) As pointed out in Section 1.5.4 (d), on several occasions fitters have removed thermowells—pockets into which a temperature-measuring device is inserted—without realizing that this would result in a leak.

(c) Section 9.2.1 (c) describes an incident in which a float came loose from a level controller in a sphere containing propane and formed a

perfect fit in the short pipe below the relief valve. When the sphere was filled completely and isolated, thermal expansion caused the 14-m-diameter sphere to increase in diameter by 0.15 m (6 in.).

14.10 SOME ACCIDENTS AT SEA

Rudyard Kipling wrote, "What do they know of England who only England know?" In the same way, what do we know about process safety if we know nothing about accidents in other industries? Here are some shipping accidents with lessons for the process industries.

More than 30 years have passed since the U.S. nuclear submarine *Thresher* sank, with the loss of 129 lives, and the reasons may have been forgotten. The immediate cause was a leak of seawater from a silver-brazed joint in the engine room. This, it is believed, short-circuited electrical equipment, causing a shutdown of the reactor. As a result, the submarine was unable to empty its ballast tanks and rise to the surface.

According to a recent report [11], the "nuclear power plant was the focus of the designers' attention; the standards used for the nuclear power plant were more stringent than those for the rest of the submarine." In the process industries' utilities, storage areas and offplots often get less attention than the main units and are involved in disproportionately more incidents.

The report continues: "The Navy had experienced a series of failures with silver-brazing, which resulted in several near-misses, indicating that the traditional quality assurance method, hydrostatic testing, was inadequate. Therefore, the Navy instructed the shipyard to use ultrasonic testing . . . on the *Thresher's* silver-brazed joints. However, the Navy failed to specify the extent of the testing required and did not confirm that the testing program was fully implemented. When ultrasonic testing proved burdensome and time-consuming, and when the pressures of the schedule became significant, the shipyard discontinued its use in favor of the traditional method. This action was taken despite the fact that 20 out of 145 joints passing hydrostatic testing failed to meet minimum bonding specifications when subject to ultrasonic testing."

In the process industries, many incidents have shown the need to tell contractors precisely what they should do and then check that they have done it. It is easy to forget this at a time of recession and economies.

Another incident occurred on a British submarine. At the time, small drain valves were used to check that the torpedo outer doors were

closed; if water came out of the drain valve, then the outer door was open. The reverse, however, was not true. On one occasion the drain valve was plugged; the inner door was opened when the outer door was also open; the submarine sank, and many sailors drowned. Many similar incidents have occurred in the process industries, for example, when testing for trapped pressure, though with less serious results. Before testing ask what will happen if the result is not what we expect it to be (Section 14.1 g).

The loss of the *Titanic* in 1912 has been the subject of many books. The loss of another luxury ship, the *Ville du Havre,* off the Newfoundland coast in 1873, as the result of a collision, is less well known. The lifeboats were difficult to detach, as the ship was newly painted and everything was stuck fast; many could not be detached in time. The life preservers, along the sides of the deck, were also stuck fast. Fifty-seven people were rescued, but 226 drowned. On chemical plants, painters have been known to paint everything in sight [12].

This disaster, like the loss of the *Thresher,* shows the importance of checking the work of contractors. It also shows the need to try out all emergency equipment from time to time, especially after maintenance, whether it is a diesel generator, an interlock, an alarm, or a lifeboat. On the *Titanic*, the most serious deficiency was lack of sufficient boats for all the passengers, but failure to try out emergency equipment added to the loss of lives. The crew had difficulty removing covers from the boats and cutting them loose. There had been no lifeboat drills, and some of the crew members did not know where to go [13].

Overheard from a woman leaving a movie theater after seeing James Cameron's *Titanic*:

> You know, that could really happen.
>
> —*Daily Telegraph* (London), Mar. 2, 1998

REFERENCES

1. W. H. Doyle, "Some Major Instrument Connected CPI Losses," Paper presented at Chemical Process Industry Symposium, Philadelphia, Pa., 1972.
2. J. A. McLean, *Loss Prevention Bulletin,* No. 110, Apr. 1993, p. 1.

3. Health and Safety Executive, *Passenger Falls from Train Doors,* Her Majesty's Stationery Office, London, 1993.
4. R. Roussakis and K. Lapp, "A Comprehensive Test Method for Inline Flame Arresters," Paper presented at AIChE Loss Prevention Symposium, San Diego, Aug. 1990.
5. R. A. McConnell, *Process Safety Progress,* Vol. 16, No. 2, Summer 1997, p. 61.
6. *Operating Experience Weekly Summary,* No. 97-10, Office of Nuclear and Safety Facility, U.S. Dept. of Energy, Washington, D.C., 1997, p. 1.
7. *Operating Experience Weekly Summary,* No. 97-12, Office of Nuclear and Safety Facility, U.S. Dept. of Energy, Washington, D.C., 1997, p. 5.
8. *Health and Safety at Work,* Vol. 19, No. 5, May 1997, p. 5.
9. *Operating Experience Weekly Summary,* No. 97-27, Office of Nuclear and Safety Facility, U.S. Dept. of Energy, Washington, D.C., 1997, p. 4.
10. S. Hall, *Railway Detectives,* Ian Allen, Shepperton, UK, 1990, p. 117.
11. *Occupational Safety Observer,* Vol. 3, No. 6, U.S. Dept. of Energy, Washington, D.C., June 1994, p. 4.
12. B. S. Vester, *Our Jerusalem,* Ariel, Jerusalem, 1950, 1988, p. 32.
13. Lord Mersey, *Report on the Loss of the S.S. Titanic,* St. Martin's Press, New York, 1990 (reprint).

Chapter 15

Static Electricity

Static electricity (static for short) has been blamed for many fires and explosions, sometimes correctly. Sometimes, however, investigators have failed to find any other source of ignition. So they assume that it must have been static even though they are unable to show precisely how a static charge could have been formed and discharged.

A static charge is formed whenever two surfaces are in relative motion, for example, when a liquid flows past the walls of a pipeline, when liquid droplets or solid particles move through the air, or when someone walks, gets up from a seat, or removes an article of clothing. One charge is formed on one surface—for example, the pipe wall—and an equal and opposite charge is formed on the other surface—for example, the liquid flowing past it.

Many static charges flow rapidly to earth as soon as they are formed. But if a charge is formed on a nonconductor or on a conductor that is not grounded, it can remain for some time. If the level of the charge, the voltage, is high enough, the static will discharge by means of a spark, which can ignite any flammable vapors that may be present. Examples of nonconductors are plastics and nonconducting liquids, such as most pure hydrocarbons. Most liquids containing oxygen atoms in the molecule are good conductors.

Even if a static spark ignites a mixture of flammable vapor and air, it is not really correct to say that static electricity caused the fire or explosion. The real cause was the leak or whatever event led to the formation of a flammable mixture. Once flammable mixtures are formed, experience shows that sources of ignition are likely to turn up. The deliberate formation of flammable mixtures should never be allowed except when the risk

of ignition is accepted—for example, in the vapor spaces of fixed-roof tanks containing flammable nonhydrocarbons (see Section 5.4).

15.1 STATIC ELECTRICITY FROM FLOWING LIQUIDS

Section 5.4.1 described explosions in storage tanks, and Section 13.3 described explosions in tank trucks, ignited by static sparks. The static was formed by the flow of a nonconducting liquid, and the spark discharges occurred *between the body of the liquid and the grounded metal containers* (or filling arms).

If a conducting liquid such as acetone or methanol flows into an ungrounded metal container, the container acquires a charge from the liquid, and a spark may occur *between the container and any grounded metal that is nearby*, as in the following incidents.

(a) Acetone was regularly drained into a metal bucket. One day the operator hung the bucket on the drain valve instead of placing it on the metal surface below the valve (Figure 15-1).

The handle of the bucket was covered with plastic. When acetone was drained into the bucket, a static charge accumulated on the acetone and on the bucket. The plastic prevented the charge from flowing to earth via the drain pipe, which was grounded. Finally a spark passed between the bucket and the drain valve, and the acetone caught fire.

Even if the bucket had been grounded, it would still have been bad practice to handle a flammable (or toxic or corrosive) liquid in an open container. It should have been handled in a closed can to prevent spillages (see Sections 7.1.3 and 12.2 c). Closed cans, how-

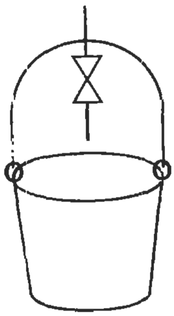


Figure 15-1. The bucket was not grounded and acquired a charge.

ever, will not prevent ignition by static electricity, as the following incidents show.

(b) A man held a 10-L metal container while it was being filled with acetone. When he tried to close the valve in the acetone line, the acetone ignited, and the fire spread to other parts of the building. The man was wearing insulating (crepe rubber) shoes, and it is believed that a static charge accumulated on the acetone, the can, and the man. When he put his hand near the valve, a spark jumped from him to the valve, which was grounded, and ignited the acetone vapor.

(c) Metal drums were occasionally filled with vinyl acetate via a 2-in.-diameter rubber hose. There was no means for grounding the drum, and the rubber hose did not reach to the bottom of the drum; the liquid splashed down from a height of 0.6 m. A few minutes after filling started, a violent explosion occurred, and the ends of the drum were blown out. One end hit a man in the legs, breaking both of them, and the other end broke another man's ankle. He was burned in the ensuing fire and died a few days later.

Note that, as in the incident described in Section 13.3, the operation had been carried out a number of times before conditions were right for an explosion to occur.

(d) Explosions have occurred because external paint prevented grounding of a drum or internal linings prevented grounding of the contents [4].

As with tanks (Section 5.4.1), explosions can also occur in grounded drums containing liquids of low conductivity if a static charge accumulates on the liquid and passes to a grounded conductor, such as a filling pipe. Reference 4 describes some incidents that have occurred. They are most likely when:

- The liquid has a low conductivity (less than 50 pS/m) and a low minimum ignition energy (less than 1 mJ).
- The vapor-air mixture in the drum is close to the optimum for an explosion. This usually occurs about midway between the lower and upper explosive limits.
- The liquid acquires a high charge by flowing through a filter, rough-bore hose, or other obstruction.

If these conditions are unavoidable, it may be necessary to inert the drum with nitrogen before filling.

15.2 STATIC ELECTRICITY FROM GAS AND WATER JETS

On a number of occasions people have received a mild electric shock while using a carbon dioxide fire extinguisher. The gas jets from the extinguishers contain small particles of solid carbon dioxide, so a charge will collect on the horn of the extinguisher and may pass to earth via the hand of the person who is holding the horn.

A more serious incident of the same sort occurred when carbon dioxide was used to inert the tanks of a ship, which had contained naphtha. An explosion occurred, killing four men and injuring seven. The carbon dioxide was added through a plastic hose 8 m long, which ended in a short brass hose (0.6 m long) that was dangled through the ullage hole of one of the tanks. It is believed that a charge accumulated on the brass hose and a spark passed between it and the tank (see Section 19.4) [1].

A few years later carbon dioxide was injected into an underground tank containing jet fuel as a tryout of a fire-fighting system. The tank blew up, killing 18 people who were standing on top of the tank. In this case the discharge may have occurred from the cloud of carbon dioxide particles.

The water droplets from steam jets are normally charged, and discharges sometimes occur from the jets to neighboring grounded pipes. These discharges are of the corona type rather than true sparks and may be visible at night; they look like small flames [2].

Discharges from water droplets in ships' tanks (being cleaned by high-pressure water-washing equipment) have ignited flammable mixtures and caused serious damage to several supertankers [3]. The discharges occurred from the cloud of water droplets and were thus "internal lightning."

A glass distillation column cracked, and water was sprayed onto the crack. A spark was seen to jump from the metal cladding on the insulation, which was not grounded, to the end of the water line. Although no ignition occurred in this case, the incident shows the need to ground all metal objects and equipment. They may act as collectors for charges from steam leaks or steam or water jets.

Most equipment is grounded by connection to the structure or electric motors. But this may not be true of insulation cladding, scaffolding,

pieces of scrap or tools left lying around, or pieces of metal pipe attached by nonconducting pipe or hose (see next item). In one case, sparks were seen passing from the end of a disused instrument cable; the other end of the cable was exposed to a steam leak.

15.3 STATIC ELECTRICITY FROM POWDERS AND PLASTICS

A powder was emptied down a metal duct into a plant vessel. The duct was replaced by a rubber hose, as shown in Figure 15-2. The flow of powder down the hose caused a charge to collect on it. Although the hose was reinforced with metal wire and was therefore conducting, it was connected to the plant at each end by short polypropylene pipes that were nonconducting. A charge therefore accumulated on the hose, a spark occurred, the dust exploded, and a man was killed.

A nonconducting hose would have held a charge. But a spark from it would not have been as big as from a conducting hose and might not have ignited the dust, though we cannot be certain. It would have been safer than an ungrounded conducting hose but less safe than a grounded conducting hose.

Hoses and ducts used for conveying explosive powders should be made from conducting material and be grounded throughout. Alternatively (or additionally) the atmosphere can be inerted with nitrogen, the ducts can be made strong enough to withstand the explosion, or an explosion vent can be provided.

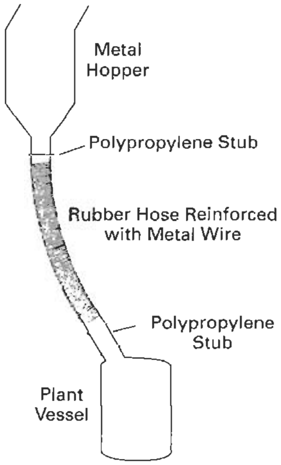


Figure 15-2. The flow of powder caused a static charge to collect on the insulated hose.

Electrostatic discharges can ignite a chemical reaction even when no air is present. For example, when a powder was dried under vacuum, electrostatic discharges produced, in the powder, a network of channels of increased conductivity. When the vacuum was broken, with nitrogen, the rise in pressure produced sudden increased sparking and a runaway decomposition of the powder. Operation under a lower vacuum prevented the ignitions, as the discharges were then more frequent and therefore less energetic and less damaging [12].

Another incident occurred in a storage bin for a granular material. The level in the bin was measured by the change in the capacity of a vertical steel cable. The measuring device was disconnected, and the cable thus became an ungrounded conductor. A charge accumulated on it, and a spark passed between the cable and the wall, about 0.3 m (1 ft) away. At the time, the level in the bin was low, and the whole of the cable was uncovered. An explosion occurred in the bin, but it was vented through a relief panel, and there was no damage. The granules were considered difficult to ignite, but the fines in them accumulated on the cable [9].

The first and third incidents are examples of hazards introduced by simple modifications (see Chapter 2). Many dust explosions caused by other sources of ignition are reviewed in Reference 10.

Note that introducing a plastic section in a pipeline so that the metal pipe beyond the section is no longer grounded can be a hazard with liquids as well as powders. On several occasions, to prevent splashing when tank trucks are filled, plastic extension pieces have been fitted to the filling arms. The extension pieces included ungrounded metal parts; charge accumulated on them and then discharged, igniting the vapor in the tank trucks [13].

Several fires have occurred when powders were added manually to vessels containing flammable atmospheres, and the use of mechanical methods of addition is recommended [5, 11]. It is better to prevent the formation of explosive mixtures by blanketing with inert gas or by lowering the temperature of the liquid. Reference 5 also describes several discharges that have occurred from plastic surfaces. For example, an operator wiped the plastic cover of an inspection lamp, approved for use in flammable atmospheres, with his glove. The cover became charged, and when it was inserted into a vessel containing a flammable atmosphere—it was an aluminum vessel that had been cleaned with sodium hydroxide solution so that hydrogen was produced—an ignition occurred. Electrical equipment for use in flammable atmospheres should

have a surface resistance of less than 1 G ohm at 50% relative humidity. The vessel should not, of course, have been inspected until it had been gas-freed.

A gasoline spillage ignited when someone attempted to sweep it up with a broom that had plastic bristles. The spillage should have been covered with foam.

Although ignitions have occurred as a result of static discharges from plastic surfaces, ". . . the number of incidents is extremely small in relation to the widespread use of plastic material" [6]. If plastic surfaces are liable to become charged and flammable mixtures are likely to be present, then the exposed area of plastic should not exceed 20 cm^2 if the ignition energy of the mixture is 0.2 mJ; less if the ignition energy is lower.

15.4 STATIC ELECTRICITY FROM CLOTHING

(a) An operator slipped on a staircase, twisted his ankle, and was absent for 17 shifts. The staircase was in good condition, and so were the operator's boots.

Many people's reaction would have been that this is another of those accidents that we can do nothing about, another occasion when "man told to take more care" appears on the accident report.

However, in the plant where the accident occurred, they were not satisfied with this easy way out. They looked into the accident more thoroughly. The injured man was asked why he had not used the handrails.

It then came to light that the handrails were covered with plastic and that anyone using them *and wearing insulating footwear* acquired an electric charge. When he touched the metal of the plant, he got a mild electric shock. The spark, of course, was not serious enough to cause any injury. But it was unpleasant. People therefore tended not to use the handrails.

For a spark to be felt, it must have an energy of at least 1 mJ. The minimum energy required to ignite a flammable mixture is 0.2 mJ, so a spark that can be felt is certainly capable of causing ignition if flammable vapor is present.

(b) We have all acquired a static charge by walking across a man-made fiber carpet (or just by getting up from our chairs) and then felt a mild shock when we touched a metal object, such as a filing cabi-

net. Similar charges can be acquired by walking across a plant floor wearing nonconducting footwear. And sparks formed in this way have been known to ignite leaks of flammable gas or vapor, especially in dry climates. However, the phenomenon is rare. It does not justify insistence on the use of conducting footwear unless leaks are common [7]. If leaks are common, action to prevent them from occurring is more effective than action to prevent them from igniting.

(c) A driver arrived at a filling station, removed the cap from the end of the filler pipe, and held it in his hand while an attendant filled the car with gasoline. The driver took off his pullover sweater, thus acquiring a charge and leaving an equal and opposite charge on the pullover, which he threw into the car. He was wearing nonconducting shoes, so the charge could not leak away to earth.

When he was about to replace the cap on the end of the filler pipe, a spark jumped from the cap to the pipe, and a flame appeared on the end of the pipe. It was soon extinguished. The flame could not travel back into the gasoline tank. The mixture of vapor and air in the tank was too rich to explode.

At one time there was concern that man-made fiber clothing might be more likely than wool or cotton clothing to produce a charge on the wearer. The incident just described shows that the static charge was produced only when the clothing was removed. When dealing with a leak, we do not normally start by removing our clothing. There is therefore no need to restrict the types of cloth used, so far as static electricity is concerned. Electrostatic sparks from people are reviewed in Reference 8.

REFERENCES

1. *Fire Journal,* Nov. 1967, p. 89.
2. A. F. Anderson, *Electronics and Power,* Jan. 1978.
3. *S. S. Mactra (ON 337004)—Report of Court No. 8057 Formal Investigation,* Her Majesty's Stationery Office, London, 1973.
4. L. G. Britton and J. A. Smith, "Electrostatic Hazards of Drum Filling," Paper presented at AIChE Loss Prevention Symposium, Minneapolis, Aug. 1987.
5. Health and Safety Executive, *Electrostatic Ignition,* Her Majesty's Stationery Office, London, 1982.

6. N. Gibson and D. J. Harper, *Journal of Electrostatics,* Vol. 11, 1981, p. 27.
7. R. W. Johnson, *Loss Prevention,* Vol. 14, 1981, p. 29.
8. B. D. Berkey, T. H. Pratt, and G. M. Williams, "Review of Literature Related to Human Spark Scenarios," Paper presented at AIChE Loss Prevention Symposium, Minneapolis, Aug. 1987.
9. L. G. Britton and D. C. Kirby, *Plant/Operations Progress,* Vol. 8, No. 3, July 1989, p. 177.
10. R. K. Eckhoff, *Dust Explosions in the Process Industries,* 2nd edition, Butterworth-Heinemann, Oxford, UK, 1997.
11. J. Bond, *Loss Prevention Bulletin,* No. 088, Aug. 1989, p. 21.
12. D. K. Davies, *Electrostatics News,* No. 5, Southampton University, UK, Spring 1966, p. 3.
13. T. H. Pratt and J. G. Atharton, *Process Safety Progress,* Vol. 15, No. 3, Fall 1996, p. 173.

Chapter 16

Materials of Construction

For him iron is as flimsy as straw, and bronze as soft as rotten wood.

—Job 41:27, *Good News Bible*

16.1 WRONG MATERIAL USED

Many incidents have occurred because the wrong material of construction was used. This has usually been the result of errors by maintenance or construction personnel or suppliers, who did not use or did not supply the materials specified. Few failures have been the result of errors by materials specialists who incorrectly specified the materials to be used.

The following incidents are typical:

(a) A titanium flange was fitted by mistake on a line carrying dry chlorine. The flange caught fire. Titanium is ideal for wet chlorine but catches fire on contact with dry chlorine. (Burning in this case means rapid combination with chlorine, not oxygen.)

In another incident, on a new plant, two flanged joints leaked an hour after chlorine was introduced. The gaskets were removed and analyzed and were found to be made from titanium although they were stamped Hastelloy, the material specified [5].

PTFE gaskets were specified for a section of plant that handled acid. As they are fragile and expensive and as an extensive series of tests using water had to be carried out during startup, temporary nitrile rubber gaskets were used during this period. You can guess what happened. One of them was left in position and corroded,

causing an acid leak. Subsequent checks showed that many more gaskets were made of the wrong material.

(b) A carbon steel valve painted with aluminum paint was used instead of a stainless steel valve. It corroded rapidly.

(c) A plug valve was supplied with a pure nickel plug instead of one made from 304L stainless steel. The valve body was made from the correct material. The valve was installed in a nitric acid line. Five hours later the plug had disappeared, and acid was escaping through the stem seal.

The manufacturers had provided a test certificate stating that the valve was made from 304L steel.

(d) During the night a valve had to be changed on a unit, which handled a mixture of acids. The fitter could not find a suitable valve in the workshop, but on looking around he found one on another unit. He tested it with a magnet and, finding it nonmagnetic, assumed it was similar to the stainless steel valves normally used. He therefore installed it. Four days later the valve was badly corroded and there was a spillage of acids.

The valve was made of Hastelloy, an alloy suitable for use on the unit where it was found but not suitable for use with the mixture of acids on the unit on which it had been installed.

(e) A tank truck, used for internal transport, looked as if it was made of stainless steel. It was therefore filled with 50% caustic soda solution. Twelve hours later the tank was empty. It was made of aluminum, and the caustic soda created a hole and leaked out.

The material of construction has now been stenciled on all tank trucks used for internal transport in the plant where the incident occurred.

(f) A small, new tank was installed with an unused branch blanked off. A month later the branch was leaking. It was then discovered that the tank had arrived with the branch protected by a blank flange made of wood. The wood was painted the same color as the tank, and nobody realized that it was not a steel blank.

(g) A leak on a refinery pump, which was followed by a fire, was due to incorrect hardness of the bolts used. Other pumps supplied by the same manufacturer were then checked, and another was found with off-specification bolts. The pump had operated for 6,500 hours before the leak occurred.

If the pump had been fitted with a remotely operated emergency isolation valve as recommended in Section 7.2.1, the leak could have been stopped quickly. Damage would have been slight. As it was, the unit shut down for five weeks.

(h) Section 9.1.6 (b) describes what happened when the exit pipe of a high-pressure ammonia converter was made from carbon steel instead of 1¼% Cr, 0.5% Mo. Hydrogen attack occurred, a hole appeared at a bend, and the reaction forces from the escaping gas pushed the converter over.

A return bend on a furnace failed after 20 years of service. It was then found that it had been made from carbon steel instead of the alloy specified.

(i) After some new pipes were found to be made of the wrong alloy, further investigation showed that many of the pipes, clips, and valves in store were also made of the wrong alloys. The investigation was extended to the rest of the plant, and the following are some examples of the findings:

1. The wrong electrodes had been used for 72 welds on the tubes of a fired heater.
2. Carbon steel vent and drain valves had been fitted on an alloy steel system.
3. An alloy steel heat exchanger shell had been fitted with two large carbon steel flanges. The flanges were stamped as alloy.

(j) Checks carried out on the materials delivered for a new ammonia plant showed that 5,480 items (1.8% of the total) were delivered in the wrong material. These included 2,750 furnace roof hangers; if the errors had not been spotted, the roof would probably have failed in service.

". . . vendors often sent without notice what they regarded as 'superior' material. Thus, if asked to supply 20 flanges in carbon steel of a given size, the vendor, if he had only 19 such flanges available, was quite likely to add a 20th of the specified size in 'superior' 2¼% Cr. When challenged the vendor was often very indignant because he had supplied 'superior,' i.e., more expensive, material at the original price. We had to explain that the 'superior' material was itself quite suitable, *if we knew about it*. If we didn't, we were quite likely to apply the welding procedures of carbon steel to 2¼% Cr steel with unfortunate results" [1].

As the result of incidents such as those described in (c) and (g) through (j) above, many companies now insist that if the use of the wrong grade of steel can affect the integrity of the plant, all steel (flanges, bolts, welding rods, etc., as well as pipes) must be checked for composition before use. The analysis can be carried out easily with a spectrographic analyzer. The design department should identify which pipelines, etc., need to be checked and should mark drawings accordingly.

Anecdotal evidence exists that some companies have relaxed their material identification programs when their suppliers' systems comply with quality standards. In view of the serious results of occasional minor errors—minor from the suppliers' point of view—it is doubtful if this is wise.

(k) The recycle of scrap to produce stainless steel has led to increases in the concentration of trace elements not covered in the steel specifications. This may lead to poorer corrosion resistance and weld quality, although so far only the nuclear power industry has reported problems. One report says, "Work on understanding the basic processes of impurity segregation in steels and the resulting embrittlement has been very important in understanding component failure problems on plant . . ." [6].

(l) Sometimes the wrong steel has been supplied as the result of misunderstanding rather than wrong labeling. Thus, suppliers have delivered CS (carbon steel) instead of C5 steel (5% Cr, 1½% Mo, 1% W); 5% Cr, ½% Mo is sometimes called P5, but this name is also used to describe 2½% Cr steel.

(m) The U.S. Department of Energy has reported that some imported nuts and bolts were substandard and failed in service, causing 61 crashes of private planes between 1984 and 1987 and a fire in a U.S. Navy destroyer [7].

(n) Creep failures have been described in furnaces (Section 10.7.2) and in a pipe (Section 9.1.6 a). After 28 years of service at 540°–600°C and a gauge pressure of 900 psi (60 bar), the studs holding a bonnet of a 28-in. valve expanded as the result of creep. The effect was similar to that produced when a nut is forced onto a stud with a thread of a different pitch. The load was held by only a few threads, the studs failed, and the bonnet separated from the body. Once one stud failed, the load on the others increased, and there was a rapid cascade of failures [14].

During design the life expectancy, due to creep or other forms of corrosion, should be estimated and examination or replacement planned. Cheap fittings, such as studs, bolts, and nuts, should be replaced in good time. Not to do so is penny-pinching and expensive in the end.

Here are two more examples of penny-pinching. The piston of a reciprocating engine was secured to the piston rod by a nut, which was locked in position by a tab washer. When the compressor was overhauled, the tightness of this nut was checked. To do this, the tab on the washer had to be knocked down and then knocked up again. This weakened the washer so that the tab snapped off in service, the nut worked loose, and the piston hit the end of the cylinder, fracturing the piston rod.

The load on a 30-ton hoist slipped, fortunately without injuring anyone. It was then found that a fulcrum pin in the brake mechanism had worked loose, as the split pin holding it in position had fractured and fallen. The bits of the pin were found on the floor.

Split pins and tab washers should not be reused but replaced every time they are disturbed. Perhaps we cannot be bothered to go to the store for a fresh supply. Perhaps there is none in the store.

16.2 HYDROGEN PRODUCED BY CORROSION

Hydrogen produced by corrosion can turn up in unexpected places, as shown by the following incidents:

(a) An explosion occurred in a tank containing sulfuric acid. As the possibility of an explosion had not been foreseen, the roof/wall weld was stronger than usual, and the tank split at the base/wall weld. The tank rose 15 m into the air, went through the roof of the building, and fell onto an empty piece of ground nearby, just missing other tanks. Fortunately no one was hurt. If the tank had fallen on the other side of the building it would have fallen into a busy street.

Slight corrosion in the tank had produced some hydrogen. The tank was fitted with an overflow pipe leading down to the ground, but no vent. So the hydrogen could not escape, and it accumulated under the conical roof. The hydrogen was ignited by welders working nearby. (Presumably some found its way out of the overflow.) [2].

The tank should have been fitted with a vent at the highest point, as shown in Figure 16-1.

Many suppliers of sulfuric acid recommend that it is stored in pressure vessels designed to withstand a gauge pressure of 30 psi (2 bar). The acid is usually discharged from tank trucks by compressed air, and if the vent is choked the vessel could be subjected to the full pressure of the compressed air.

(b) Hydrogen produced by corrosion is formed as atomic hydrogen. It can diffuse through iron. This has caused hydrogen to turn up in unexpected places, such as the insides of hollow pistons. When holes have been drilled in the pistons, the hydrogen has come out and caught fire [3].

In another case, acidic water was used to clean the inside of the water jacket that surrounded a glass-lined vessel. Some hydrogen diffused through the wall of the vessel and developed sufficient pressure to crack the glass lining.

Corrosion uses up oxygen, and this has caused tanks to collapse (see Section 5.3 d) and persons to be overcome when entering a vessel (see Section 11.1 d).

(c) The sudden failure of six bonnet studs on an 8-in. valve caused a release of hydrogen fluoride, which killed two men and hospitalized ten others. The failure was the result of hydrogen-assisted stress corrosion cracking. In this phenomenon, hydrogen, produced

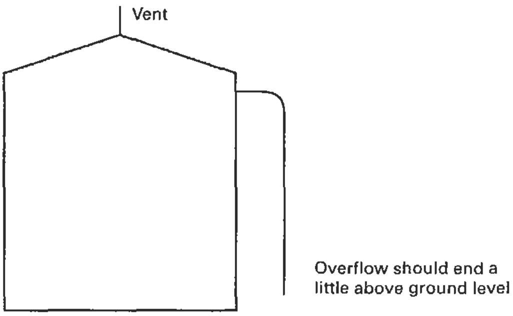


Figure 16-1. Acid tanks should be fitted with a high-point vent, as well as an overflow, so that hydrogen can escape.

by corrosion, migrates to flaws in areas of high tensile stress, where it lowers the energy needed for cracks to grow. When the cracks reach a critical size, the equipment fails suddenly. The grade of steel used in this case was unsuitable; Reference 8 lists the types that should be used.

16.3 OTHER EFFECTS OF CORROSION

Corrosion usually results in a leak or failure of a support because a vessel or support gets too thin. It is then not strong enough to withstand the pressure or load. However, rust can cause failure in another way. It occupies about seven times the volume of the steel from which it was formed. When rust occurs between two plates that have been bolted or riveted together, a high pressure develops. This can force the plates apart or even break the bolts or rivets (see Section 9.1.2 g). Corrosion of the reinforcement bars in concrete can cause the concrete to crack and break away.

16.4 LOSS OF PROTECTIVE COATINGS

Aluminum pump impellers are often used to pump fluorinated hydrocarbon refrigerants. If the impeller rubs against the casing, the protective film of aluminum oxide is removed, and combined with the local heating produced by the rubbing, which allows the aluminum to react with the refrigerant, the impeller may disappear. Contact between the impeller and the casing may be a result of worn bearings, which in turn are the result of compressor surges, so the reasons for any surging should be investigated [4].

A special type of high-pressure joint incorporated copper gaskets. A change was made to aluminum after laboratory tests showed no sign of reaction with the process material. The gaskets normally lasted for many years, but one failed after a few days. It was then found that the man who installed it, anxious to do a good job, had cleaned the gasket immediately before installing it. In doing so he removed the film of oxide, and the aluminum now dissolved in the process liquid. It was usual to clean the gaskets a few days before they were installed. Though it was not realized at the time, this allowed a fresh oxide film to form.

A change was made back to copper. It is more user friendly than aluminum and will tolerate cleaning or scratching of the surface.

16.5 SOME OTHER INCIDENTS CAUSED BY CORROSION

(a) An oil company took a section of plant out of use and, due to an oversight, did not remove process materials from all the pipework. For 18 years a pipe was left with a mixture of hydrogen fluoride and benzene boxed up inside it. Finally, the walls became so thin that they burst, and ten men were taken to the hospital suffering from the effects of acid gas [9].

(b) A plant made an evaporator for liquid nitrogen by running hundreds of meters of copper piping through a steel tank filled with water. Although the steel was painted, it corroded right through in six months as the result of galvanic corrosion—that is, the steel and the copper formed an electrolytic cell. Paint never gives 100% cover, and if 1% of the steel was uncovered, all the current would have passed though this area, and its corrosion rate would have been increased 100 times. Painting the copper, which did not corrode, would be more effective than painting the steel! [10].

This incident illustrates the hazards of do-it-yourself engineering by people who do not fully understand the properties of the materials they are using.

(c) Minute amounts (up to 300 $\mu g/m^3$) of mercury in natural gas have caused brittle failure of certain alloys. Valves have failed as a result. In addition, reaction of the mercury with ammonia can produce explosive compounds [11].

(d) Some catalyst tubes in a reactor failed as a result of chloride-induced stress corrosion cracking soon after startup. A materials expert, called in to investigate, found that all the failures had occurred in one corner of the reactor, that men had been working on the roof, day and night, for several weeks after the tubes had been fitted, that this area of the roof could not be seen from the rest of the plant, and that to reach the nearest restroom the men had to negotiate three ladders [12].

Reference 13 describes some other corrosion problems.

16.6 FIRES

We know that metals, especially aluminum (see Section 10.1), can be affected by fire, but we do not usually consider the possibility that they

will burn. However, some metals, including titanium, will burn when powdered or finely divided, and bulk titanium will also burn. Three titanium heat exchangers were set alight and destroyed by burning operations. In one case, ignition was started by direct contact with the torch and in the other two cases by contact with hot slag [15]. Great care is needed if welding or burning is carried out anywhere near titanium equipment.

16.7 CHOOSING MATERIALS

In choosing materials of construction, we have to compromise between various factors. Kirby [16] uses the acronym SHAMROCK to summarize and remember them.

S = Safety: what are the consequences of failure? If they are serious, a more resistant material than usual may be justified. For example, on a plant where leaking water would react violently with process materials, the water lines were made from a grade of steel resistant to stress corrosion cracking (from the chloride in the cooling water) as well as rust.

H = History: if a plant has used material successfully for many years, and the staff members know its strengths and limitations, how to weld it, etc., hesitate before making a change. For example, a fiberglass-reinforced plastic had given excellent service for many years; when another composite from the same company, with the same name but a different number, was used instead, it failed overnight.

A = Availability: before a salesman sells you the latest wonder-working material, ask how easy it will be to get replacement supplies in a hurry.

M = Maintenance: a plant engineer saved $10,000 per year by no longer neutralizing the slightly acidic cooling water. In time, rust formation in 30 jacketed reactors increased reaction times by 25%. I have known several engineers who gained a reputation for efficiency by similar measures, including neglecting maintenance, and then left their successors to pick up the tab.

R = Reparability: a plant bought some vessels with a new type of plastic lining instead of the one they had used for many years. The new material had better temperature resistance than the old, but when it did need repair, the patches would not stick. In time the problems were overcome, but reparability should have been considered before the change was made.

O = Oxidizing/reducing nature of process fluids: in acidic solutions, this affects the choice of alloys.

C = Cost: an important consideration, but look at lifetime costs, including maintenance, not just at initial costs. Penny-pinching (Section 16.1 n) is rarely worthwhile.

K = Kinetics of corrosion mechanisms: unless we understand these, we will not know which materials will be suitable and which will not.

REFERENCES

1. G. C. Vincent and C. W. Gent, *Ammonia Plant Safety*, Vol. 20, 1978, p. 22.
2. *Chemical Safety Summary*, No. 192, Chemical Industries Association, London, Oct./Dec. 1977.
3. *Case Histories of Accidents in the Chemical Industry*, No. 1807, Manufacturing Chemists Association, Washington, D.C., Apr. 1975.
4. R. Stevens, *Plant/Operations Progress*, Vol. 4, No. 2, Apr. 1985, p. 68.
5. *Loss Prevention Bulletin*, No. 097, Feb. 1991, p. 9.
6. B. Eyre, *Atom*, No. 407, Oct. 1990, p. 11.
7. *DOE Quality Alert*, Bulletin No. DOE/EH-0266, U.S. Dept. of Energy, Washington, D.C., Aug. 1992.
8. *Loss Prevention Bulletin*, No. 089, Oct. 1989, p. 27.
9. *Health and Safety at Work*, Vol. 14, No. 6, June 1990, p. 4.
10. M. Turner, *The Chemical Engineer*, No. 468, Jan. 1990, p. 28.
11. S. M. Williams, *Plant/Operations Progress*, Vol. 10, No. 4, Oct. 1991, p. 189.
12. M. Turner, *The Chemical Engineer*, No. 492, Mar. 14, 1991, p. 40.
13. *Corrosion Awareness—A Three-Part Videotape Series*, Gulf Publishing Co., Houston, Texas, 1991.
14. S. J. Brown, *Plant/Operations Progress*, Vol. 6, No. 1, Jan. 1987, p. 20.
15. G. E. Mahnken and M. T. Rook, *Process Safety Progress*, Vol. 16, No. 1, Spring 1997, p. 54.
16. G. N. Kirby, *Chemical Engineering Progress*, Vol. 92, No. 6, June 1996, p. 38.

Chapter 17

Operating Methods

> . . . people place their faith in systems either because they're new (so they simply must be good) or because they're old and have worked a long time.
>
> —Wendy Grossman, *Daily Telegraph* (London). July 29, 1997

This chapter describes some accidents that occurred because operating procedures were poor. It does not include accidents that occurred because of defects in procedures for preparing equipment for maintenance or vessels for entry. These are discussed in Chapters 1 and 11.

17.1 TRAPPED PRESSURE

Trapped pressure is a familiar hazard in maintenance operations and is discussed in Section 1.3.6. Here we discuss accidents that have occurred as a result of process operation.

Every day, in every plant, equipment that has been under pressure is opened up. This is normally done under a work permit. One man prepares the job, and another opens up the vessel. And it is normally done by slackening bolts so that any pressure present will be detected before it can cause any damage—provided the joint is broken in the correct way, described in Section 1.5.1.

Several fatal or serious accidents have occurred when one man has carried out the whole job—preparation and opening up—and has used a quick-release fastening instead of nuts and bolts. One incident, involving a tank truck, is described in Section 13.5. Here is another:

A suspended catalyst was removed from a process stream in a pressure filter. After filtration was complete, the remaining liquid was blown out of the filter with steam at a gauge pressure of 30 psi (2 bar). The pressure in the filter was blown off through a vent valve, and the fall in pressure was observed on a pressure gauge. The operator then opened the filter for cleaning. The filter door was held closed by eight radial bars, which fitted into U-bolts on the filter body. The bars were withdrawn from the U-bolts by turning a large wheel, fixed to the door. The door could then be withdrawn.

One day an operator started to open the door before blowing off the pressure. As soon as he opened it a little, it blew open and he was crushed between the door and part of the structure and was killed instantly.

In situations such as this, it is inevitable that sooner or later an operator will forget that he has not blown off the pressure and will attempt to open up the equipment while it is still under pressure. On this particular occasion the operator was at the end of his last shift before starting his vacation.

As with the accidents described in Section 3.2, it is too simple to say that the accident was due to the operator's mistake. The accident was the result of a situation that made it almost inevitable.

Whenever an operator has to open up equipment that has been under pressure:

(a) The design of the door or cover should allow it to be opened about ¼ in. (6 mm) while still capable of carrying the full pressure, and a separate operation should be required to release the cover fully. If the cover is released while the vessel is under pressure, then this is immediately apparent, and the pressure can blow off through the gap, or the cover can be resealed.

(b) Interlocks should be provided so that the vessel cannot be opened up until the source of pressure is isolated and the vent valve is open.

(c) The pressure gauge and vent valve should be visible to the operator when he or she is about to open the door or cover [1].

Pressure can develop inside drums, and then when the lid is released, it may be forcibly expelled and injure the person releasing it. Most of the incidents reported have occurred in waste drums where chemicals have reacted together. For example, nitric acid has reacted with organic com-

pounds. Acids may corrode drums and produce hydrogen. Rotting organic material can produce methane. Materials used for absorbing oil spillages can expand to twice their original volume. Some absorbent was placed in drums with waste oil; the drums were allowed to stand for two days before the lids were fitted, and 10% free space was left, but nevertheless pressure developed inside them. If drums are found to be bulged, lid-restraining devices should be fitted before they are opened or even moved [9].

17.2 CLEARING CHOKED LINES

(a) A man was rodding out a choked ¼-in. line leading to an instrument (Figure 17-1a). When he had cleared the choke he found that the valve would not close and he could not stop the flow of flammable liquid. Part of the unit had to be shut down.

Rodding out *narrow bore* lines is sometimes necessary. But before doing so, a ball valve or cock should be fitted on the end (Figure 17-1b). It is then possible to isolate the flow when the choke has been cleared, even if the original valve will not close.

(b) Compressed air at a gauge pressure of 50 psi (3.4 bar) was used to clear a choke in a 2-in. line. The solid plug got pushed along with such force that when it reached a slip-plate (spade), the slip-plate was knocked out of shape, rather like the one shown in Figure 1-6.

On another occasion, a 4-in.-diameter vertical U-tube, part of a large heat exchanger, was being cleaned mechanically when the cleaning tool, which weighed about 25 kg, stuck in the tube. A supply of nitrogen at a gauge pressure of 3,000 psi (200 bar) was available, so it was decided to use it to try to clear the choke. The

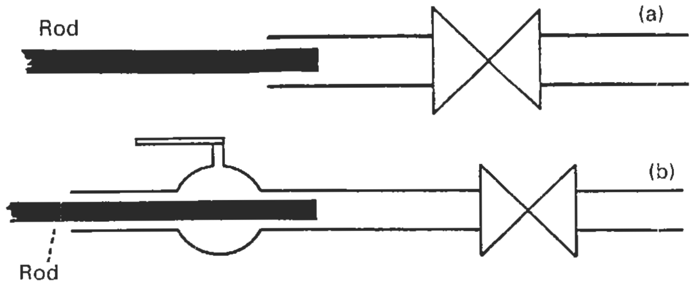


Figure 17-1. The wrong (a) and right (b) ways of clearing a choked line.

tool shot out of the end of the U-tube and came down through the roof of a building 100 m away.

Gas pressure should never be used for clearing choked lines.

(c) A 1-in. line, which had contained sulfuric acid, was choked. It was removed from the plant, and an attempt was made to clear it with water from a hose. A stream of acid spurted 5 m into the air, injuring one of the men working on the job. Those concerned either never knew or had forgotten that much heat is evolved when sulfuric acid and water are mixed.

(d) When clearing chokes in drain lines, remember that there may be a head of liquid above the choke. The following incident illustrates the hazards:

The drain (blowdown) line on a boiler appeared to be choked. It could not be cleared by rodding (the choke was probably due to scale settling in the base of the boiler), so the maintenance foreman pushed a water hose through the drain valve and turned on the water. The choke cleared immediately, and the head of water left in the boiler pushed the hose out of the drain line and showered the foreman with hot water. Although the boiler had been shut down for 15 hours, the water was still at 80°–90°C and scalded the foreman.

Clearing the choke should not have been attempted until the temperature of the water was below 60°C, the foreman should have worn protective clothing, and if possible a second valve should have been fitted to the end of the drain line as described in (a) above. The accumulation of scale suggests that the water treatment was not adequate [3].

(e) An acid storage tank was emptied so that the exit valve could be changed. The tank was then filled with acid, but the new valve seemed to be choked. After the tank had been emptied again (quite a problem, as the normal exit line was not available), the staff found that the gasket in one of the flanged joints on the new valve had no hole in it!

(f) An operator who tried to clear a choke in a pump with high-pressure steam was killed when the seal gave way and sprayed him with a mixture of steam and a corrosive chemical (2, 4-dichlorophenol). He was not wearing protective clothing. The seal was the wrong type, was badly fitted, and had cracked. When the company was prosecuted, its defense was that the operator should have notified

the maintenance department and not attempted to clear the choke himself; had the managers known that operators tried to clear blockages by themselves, they would not have condoned the practice. However, this is no excuse; it is the responsibility of managers to keep their eyes open and know what goes on.

The company had set up a computer system designed to pinpoint any equipment that needed replacing, but eight months before the accident it was found to be faulty and was shut down. The judge said, "You don't need an expert armed with a computer to know what will happen when the wrong type of seal is mixed with high-pressure steam" [4].

17.3 FAULTY VALVE POSITIONING

Many accidents have occurred because operators failed to open (or close) valves when they should have. Most of these incidents occurred because operators forgot to do so, and such incidents are described in Sections 3.2.7, 3.2.8, 13.5, and 17.1. In this section we discuss incidents that occurred because operators did not understand why valves should be open (or closed).

(a) As described in Section 3.3.4 (c), the emergency blowdown valves on a plant were kept closed by a hydraulic oil supply. One day the valves opened, and the plant started to blow down. It was then discovered that, unknown to the manager and contrary to instructions, the foreman had developed the practice of isolating the oil supply valve "in case the supply pressure in the oil system failed." This was a most unlikely occurrence and much less likely than the oil pressure leaking away from an isolated system.

(b) The air inlet to a liquid-phase oxidation plant became choked from time to time. To clear the choke, the flow of air was isolated, and some of the liquid in the reactor was allowed to flow backward through the air inlet and out through a purge line, which was provided for this purpose (Figure 17-2).

One day the operator closed the remotely operated valve in the air line but did not consider it necessary to close the hand valve as well, although the instructions said he should. The remotely operated valve was leaking, the air met the reactor contents in the feed line, and reaction took place there. The heat developed caused the line to fail, and a major fire followed.

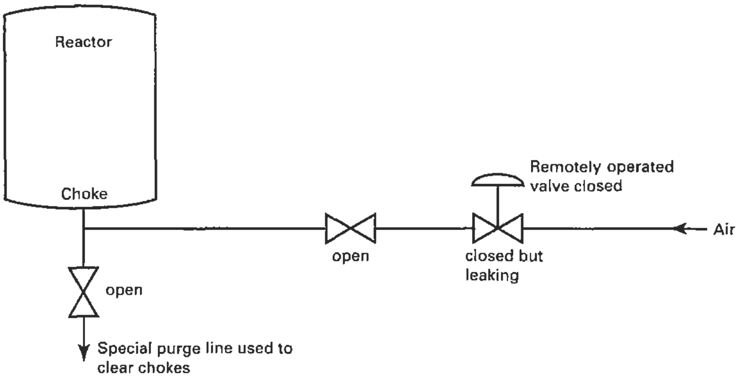


Figure 17-2. Liquid purge burned in the drain line.

The air line should have been provided with remotely operated double block and bleed valves, operated by a single button.

Other incidents in which operators relied on automatic valves and did not back them up with hand valves are described in Sections 14.6 and 17.5 (c).

(c) An engineer flew from Japan to Korea to investigate a customer's complaint: there must be something wrong with the crude oil supplied, as no distillate was produced. Within 30 minutes he found a valve in the vacuum system incorrectly closed [10].

17.4 RESPONSIBILITIES NOT DEFINED

The following incident shows what can happen when responsibility for plant equipment is not clearly defined and operators in different teams, responsible to different supervisors, are allowed to operate the same valves.

The flarestack shown in Figure 17-3 was used to dispose of surplus fuel gas, which was delivered from the gasholder by a booster through valves C and B. Valve C was normally left open because valve B was more accessible.

One day the operator responsible for the gasholder saw that it had started to fall. He therefore imported some gas from another unit. Nevertheless, a half hour later the gasholder was sucked in.

Another flarestack at a different plant had to be taken out of service for repair. An operator at this plant therefore locked open valves A and B so

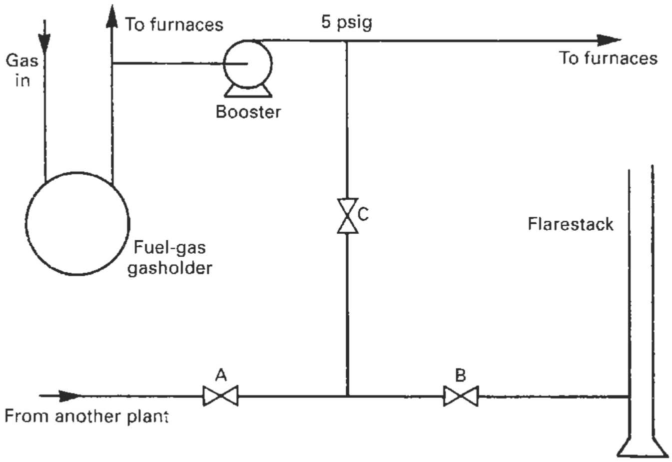


Figure 17-3. Valve B was operated by different operators.

that he could use the "gasholder flarestack." He had done this before, though not recently, and some changes had been made since he last used the flarestack. He did not realize that his action would result in the gasholder emptying itself through valves C and B. He told three other men what he was going to do, but he did not tell the gasholder operator. He did not know that this man was concerned.

Responsibility for each item of equipment should be clearly defined at the supervisor, foreman, and operator levels, and only the people responsible for each item should operate it. If different teams are allowed to operate the same equipment, then sooner or later an incident will occur.

Section 10.7.2 (c) describes a similar incident.

17.5 COMMUNICATION FAILURES

This section describes some incidents that occurred because of failures to tell people what they needed to know, because of failures to understand what had been told, and because of misunderstandings about the meanings of words.

(a) A maintenance foreman was asked to look at a faulty cooling water pump. He decided that, to prevent damage to the machine, it was essential to reduce its speed immediately. He did so, but did not tell any of the operating team members straight away. The cooling water rate fell, the process was upset, and a leak developed on a cooler.

(b) A tank truck, which had contained liquefied petroleum gas, was being swept out before being sent for repair. The laboratory staff was asked to analyze the atmosphere in the tanker to see if any hydrocarbon was still present. The laboratory staff regularly analyzed the atmosphere inside LPG tank trucks to see if any oxygen was present. Owing to a misunderstanding, they assumed that an oxygen analysis was required on this occasion and reported over the telephone, "None detected." The operator assumed that no hydrocarbon had been detected and sent the tank truck for repair.

Fortunately the garage had its own check analysis carried out. This showed that LPG was still present—actually more than 1 ton of it.

For many plant control purposes, telephone results are adequate. But when analyses are made for safety reasons, results should be accepted only in writing.

(c) A batch vacuum still was put on stand-by because there were some problems in the unit that took the product. The still boiler was heated by a heat transfer oil, and the supply was isolated by closing the control valve. The operators expected that the plant would be back on line soon, so they did not close the hand isolation valves, and they kept water flowing through the condenser. However, the vacuum was broken, and a vent on the boiler was opened.

The problems at the downstream plant took much longer than expected to correct, and the batch still stayed on stand-by for five days. No readings were taken, and when recorder charts ran out, they were not replaced.

The heat transfer oil control valve was leaking. Unknown to the operators, the boiler temperature rose from 75°C to 143°C, the boiling point of the contents. Finally, bumping in the boiler caused about 0.2 ton of liquid to be discharged through the vent.

Other incidents that occurred because operators relied on automatic valves and did not back them up with hand valves are described in Sections 14.6 and 17.3 (b). In this incident the point to be emphasized in addition is that the operators were not clear on the difference between a stand-by and a shutdown. No maximum period for stand-by was defined. And no readings were taken during periods on stand-by. Plant instructions should give guidance on both these matters.

(d) Designers often recommend that equipment is "checked" or "inspected" regularly. But what do these words mean? Designers should state precisely what tests should be carried out and what they hope to determine by the test.

In 1961 a brake component in a colliery elevator failed, fortunately without serious consequences. An instruction was issued that all similar components should be examined. It did not say how or how often. At one colliery the component was examined in position but was not removed for complete examination and was not scheduled for regular examination in the future.

In 1973 it failed, and 18 men were killed [2].

(e) Under the UK Ionizing Radiation (Sealed Sources) Regulations, all sealed radioactive sources must be checked by an authorized person "each working day" to make sure that they are still in position.

Following an incident at one plant, it was found that the plant took this to mean that the authorized person must check the presence of the sources on Mondays to Fridays but not on weekends. However, "each working day" means each day the radioactive source is working, not each day the authorized person is working!

(f) Teams develop their own shorthand. It is useful, but it can also lead to misunderstandings. On a new unit, the project team had to order the initial stocks of materials. One member of the team, asked to order some TEA, ordered some drums of tri-ethylamine. He had previously worked on a plant where tri-ethylamine was used, and it was called TEA. The manager of the new unit ordered a continuing supply of drums of tri-ethanolamine, the material actually needed and called TEA on the plant where he had previously worked. The confusion was discovered by an alert storeman who noticed that two different materials with similar names had been delivered for the same unit, and he asked if both were really required.

On other occasions, the wrong material has been delivered because prefixes such as n- or iso- were left off when ordering.

(g) A low pumping rate was needed during startup, and so the designer installed a kick-back line. For unknown reasons it fell out of use—perhaps it was not possible to operate at a low enough rate even with the kick-back in use—and instead the operators controlled the level in the suction vessel by switching the pump on and off. The control room operator watched the level and asked the outside

operators over a loudspeaker to start up and shut down the pump as required. The two outside operators worked as a team; both could do every job, and they shared the work. One day the control room operator asked for the pump to be shut down. Both outside operators were some distance away; each assumed that the other would be nearer and would shut it down. Neither shut it down, the suction vessel was pumped dry, and the pump overheated and caught fire.

Teamworking, in which everybody can do a job, can easily deteriorate into a system where nobody does it.

17.6 WORK AT OPEN MANHOLES

It was the practice on one plant to remove the manhole cover from a vessel containing warm toluene, inside a building, in order to add a solid. A change in the composition of the feedstock, not detected by analysis, resulted in the emission of more vapor than usual, and the operator was killed. Afterward it was found that the ventilation system was "poorly designed, badly installed, and modified somewhat ineffectively. In addition there appeared to have been no scheduled maintenance of the ventilation system, which was subsequently in an ineffective condition."

It is bad practice to carry out operations at open manholes when flammable or toxic vapors may be present. (Another incident was described in Section 3.3.4 a.) Whenever possible, operations should be carried out in the open air or in open-sided buildings. Gas detectors should be installed if vapors are liable to leak into closed buildings.

Many ventilation systems are part of the protective equipment of the plant (see Chapter 14), and like all protective equipment, they should be tested regularly against agreed performance criteria.

17.7 ONE LINE, TWO DUTIES

The following incident shows the hazards of using the same line for different materials. The cost of an extra line is well repaid if it prevents just one such incident.

An operator made up a solution of hydrogen peroxide (1–3%) in a make-up tank. His next job was to pump the solution into another vessel. A branch of the transfer line led to a filter, and the valve in this line had been left open (following an earlier transfer of another material). Some of the solution went into the filter. When the operator realized what was

happening, he closed the filter inlet valve but did not remove the solution that was in the filter; he did not know that it would decompose on standing. There was no relief valve on the filter, and about 12 hours later the pressure broke the head bolts and blew the head off the filter. After the explosion, separate lines and pumps were installed for the two duties, a relief valve was fitted to the filter, and the hazards of hydrogen peroxide were explained to the operators [5]—all actions that could have been taken beforehand (see also Section 20.2.1).

17.8 INADVERTENT ISOLATION

(a) The compressed air supply to a redundant tank was isolated so that the tank could be removed. No one realized that the compressed air supply to a sampling device on a vent stack came from the same supply.

When a service line supplies plant items that have no obvious connection with each other, it is good practice to fix a label on or near the valves, listing the equipment that is supplied. Alternatively, each item can be supplied by independent lines.

(b) A manganese grinding mill was continually purged with nitrogen to keep the oxygen content below 5%; an oxygen analyzer sounded an alarm if the oxygen content was too high. A screen became clogged with fine dust, and before clearing it the maintenance team members isolated the power supply. They did not know that the switch also isolated the power supply to the nitrogen blanketing equipment and to the oxygen analyzer. Air leaked into other parts of the plant undetected, and an explosion occurred.

As this incident shows, operators and maintenance workers may know how individual items of equipment work but may not understand the way they are linked together. In addition, air entered the plant because a blind flange had not been inserted (a common failing; see Section 1.1), and the screen became clogged because it was finer than usual. Changing the screen size was a modification, but its consequences had not been considered beforehand—another common failing (see Chapter 2) [6].

17.9 INCOMPATIBLE STORAGE

Two incompatible chemicals were kept in the same store; if mixed they became, in effect, a firework, easily ignited. One of the chemicals

was stored in cardboard kegs on a shelf close to a hot condensate pipe. As it was known to decompose at 50°C, the electrical department staff members were asked to disconnect the power supply to the steam boiler, but instead of doing so they merely turned the thermostat to zero. The kegs ruptured, and the chemical fell onto the second chemical, which was stored in bags immediately below. A fire occurred, followed by an explosion. The source of ignition was uncertain, but a falling lid may have been sufficient. Fire fighting was hampered by a shortage of water, which had been known to the company for four years.

The company had received advice on the storage of incompatible chemicals, but no chemist or chemical engineer was involved, and one of the chemicals was classified incorrectly [7].

17.10 MAINTENANCE—IS IT REALLY NECESSARY?

Suppose I found that my car alternator was not charging and took the car to a garage with an instruction to change the alternator. When I got it back, with a new alternator fitted, the fault would probably be cured. But the fault might have been a slack fan belt, a sticking or worn brush, or something else that could be put right for a fraction of the cost of a replacement alternator. These minor faults would probably have been put right when the alternator was changed and would have hidden the real cause of the fault. I would have paid a high and unnecessary price, and the unnecessary maintenace may have introduced a few new faults.

In the same way, if we do not carry out some simple diagnostic work first, some of the maintenance work we carry out on our plants may be unnecessary. Process operators, with the best of intentions, often say what they think is wrong; for example, if a pump is not working correctly they ask the maintenance team to check or clean the suction strainer. Sometimes the strainer is found to be clean, or the pump is no better after the strainer has been cleaned. We then find that there is a low level in the suction tank, the suction temperature is too high, the impeller is corroded, or a valve is partially shut.

Another example: a high-level alarm sounds. The tank could not possibly be full, so the operators ask the instrument maintenance department staff members to check the level measurement. After they have done so and shown that it is correct, further investigation shows that an unforeseen flow has taken place into the tank (and perhaps the tank overflows: see Section 3.3.2 a).

A third example: a heat exchanger is not giving the heat transfer expected. The maintenace team is asked to clean the tubes. When it withdraws the bundle, there is only a sprinkling of dust. We then find that the inlet temperatures or flows have changed, but no one calculated the effect on heat transfer, and no one expected that it would be so great.

Maintenance is expensive (and hazardous). A little questioning before work is carried out might save money, reduce accidents, and get the plant back on line sooner. It might also show a need for more diagnostic information: a pressure gauge here, a temperature point there [8].

17.11 AN INTERLOCK FAILURE

Interlocks can fail because they have been disarmed (that is, made inoperative), their set-points have been changed, or they are never tested, as described in Section 14.5. They can also fail as the result of errors in operation and design, as in the following incident.

A vessel was fitted with a simple mechanical interlock: a horizontal pin fitted into a slot in the vessel lid; the lid could not be moved sideways until the pin was withdrawn (Figure 17-4). Movement of the pin was controlled by a solenoid. The solenoid could not be activated and the pin withdrawn until various measurements, including the temperature and level of the liquid in the vessel, were within specified ranges.

Nevertheless the lid was moved, although the measurements were not correct. Several possible explanations were considered.

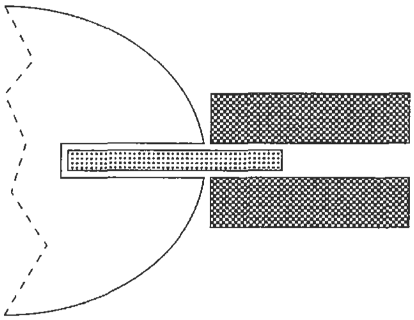


Figure 17-4. A simple mechanical interlock: the lid could not be moved until the pin was withdrawn from the slot.

1. The pin might have been seized inside the solenoid. Unfortunately the operator, believing this to be the case, had squirted a lubricant into the solenoid chamber before any investigation could be carried out. A vertical pin would have been less likely to stick.
2. The operator, believing that all measurements were correct, might have assumed that the system was faulty and inserted a thin strip of metal into the end of the slot and moved the pin back into the solenoid. He denies doing this but admits that he did not check the temperature and level readings to make sure they were correct before trying to move the lid.

   In the original design, the pin fit into a hole, but the hole was changed to a slot so the operator could see the position of the pin. At the time no one realized that this made it possible for someone to move the pin by hand, another example of the unseen results of a plant modification. To prevent this, the slot could have been covered by a sheet of transparent plastic.
3. The connection between the temperature and level measurements and the solenoid was not hardwired but went through the plant control computer. A software error might have caused the solenoid to be activated when it should not have been. The system had been in use without problems for many years, but a slight change in, for example, the order in which signals are received and processed, can result in a fault that has been lying in waiting like a time bomb for many years. Many people believe that safety interlocks should be hardwired rather than software-based (see Chapter 20). If they are software-based, they should be independent of the control system.

17.12 EMULSION BREAKING

In 1968 there was a discharge of oil vapor and mist followed by a devastating explosion in the Netherlands. The release of vapor that caused the explosion was due to a sort of foamover (Section 12.2), but the mechanism was not the usual one. In a normal foamover, a layer of heavy oil, above a water layer, is heated above 100°C. The heat gradually travels through the oil to the water. When the water boils, the steam lifts up the oil, thus reducing the pressure on the water so that it boils more vigorously. The mixture of steam and oil may blow the roof off the storage tank. Foamovers can also occur if oil, above 100°C, is added to a tank containing a water layer.

In the Netherlands incident, there were two layers in the slops tank, which was almost full. The lower layer was a stable emulsion of water in heavy oil; the upper layer was a mixture of oils with an initial boiling point of 60°C. The steam supply to the heating coils was cracked open, and the temperature of the emulsion gradually rose. When it reached 100°C, the emulsion split into water and oil layers. The oil mixed with the upper oil layer and heated it rapidly. The lighter components vaporized, and a mixture of oil vapor and mist was expelled from the tank. The escaping cloud was ignited, probably by one of the plant furnaces, and the resulting explosion caused extensive damage. Two people were killed, ten hospitalized, and about 70 were slightly injured. There was some damage outside the plant site.

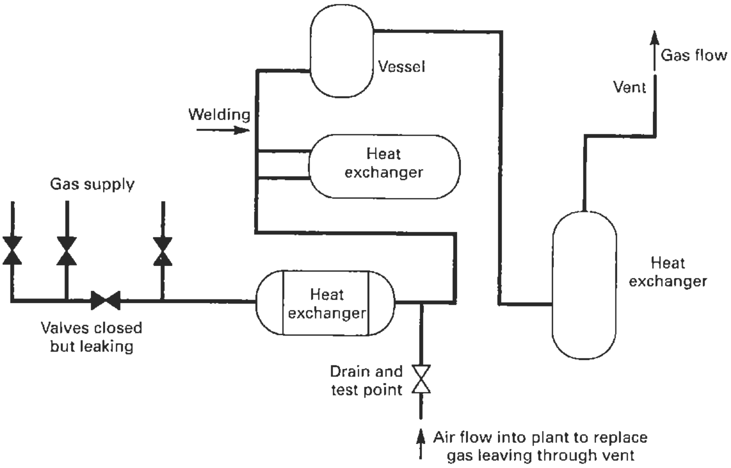
According to the official report [11], no one had ever realized before that an emulsion layer could suddenly split and give rise to a sudden eruption of hydrocarbon mist. No recommendations were made in the report. The authors presumably assumed that the recommendations were obvious and now that the cause of the explosion is known, everyone will check any tanks in which emulsion layers might form, and if they find any they will either segregate the emulsion layers, keep them at the same temperature as the overlying oil layers (by circulating the tanks), or keep them well below the temperature at which the emulsions will split. It is also clear that slops tanks should not be heated unless it is essential to do so.

17.13 CHIMNEY EFFECTS

Chimneys are common, and we all know how they work, but chimney effects in plants often take us by surprise. We fail to apply familiar knowledge because it seems to belong to a different sphere of thought, as in the following incidents.

(a) A distillation column was emptied, washed out, and purged with nitrogen. A manhole cover at the base was removed. While two men were removing the manhole cover at the top of the column, one of them was overcome. The other pulled him clear, and he soon recovered. It seems that due to a chimney effect, air entered the base of the column and displaced the lighter nitrogen [12].

(b) A hydrogen line, about 12 in. diameter, had to be repaired by welding. The hydrogen supply was isolated by closing three valves in parallel (one of which was duplicated) (Figure 17-5). The line was

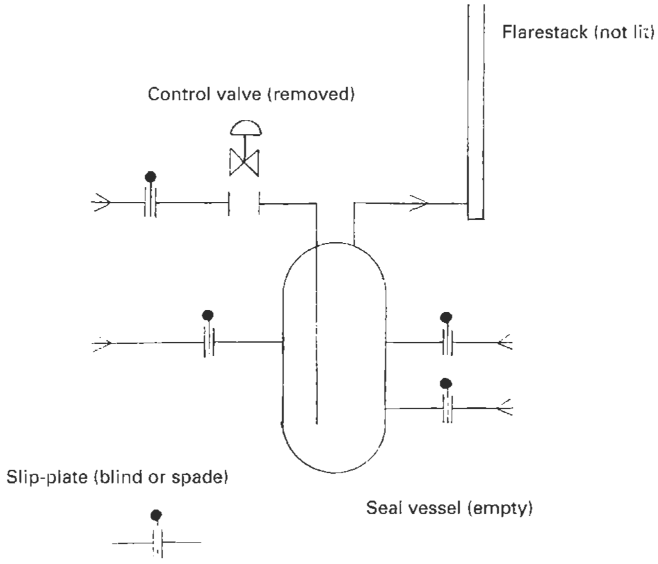


(Reproduced with permission of the American Institute of Chemical Engineers. Copyright © 1995 AIChE. All rights reserved.)

Figure 17-5. Simplified diagram of plant, showing why hydrogen gas was not detected at the drain point.

purged with nitrogen and was tested at a drain point before welding started to confirm that no hydrogen was present. When the welder struck his arc, an explosion occurred, and he was injured. The investigation showed that two of the isolation valves were leaking. It also showed why the hydrogen was not detected at the drain point: the drain point was at a low level, and air was drawn through it into the plant to replace gas leaving through a vent. The source of ignition was sparking, which occurred because the welding return lead was not securely connected to the plant (another familiar problem) [13].

(c) A flarestack and its associated seal vessel were being prepared for maintenance. The seal vessel was emptied, and all inlet lines were slip-plated (blinded). A control valve located in one of the inlet lines, between the vessel and one of the spades, was removed (Figure 17-6). Five minutes later, an explosion occurred inside the equipment. Thirty seconds later, there was a second explosion, and flames came out of the opening where the control valve had been. As the result of the chimney effect, air had entered the system, and a mixture of air and vapor had moved up the stack. The source of ignition was probably another flarestack nearby [14].



(Reproduced with permission of the American Institute of Chemical Engineers. Copyright © 1995 AIChE. All rights reserved.)

Figure 17-6. When the control valve was removed, a chimney effect caused air to enter the system, and an explosion occurred.

The flare system should have been purged with nitrogen before the lines were spaded or the control valve removed. At the very least the open end should have been blanked as soon as the valve was removed.

The incident also shows the importance of placing spades as near as possible to the equipment that is to be isolated, particularly when a vessel is to be entered. Valves should not be left between a slip-plate and the vessel, as liquid can then be trapped between the valve and the slip-plate and enter the vessel if the valve leaks or is opened.

REFERENCES

1. T. A. Kletz, *An Engineer's View of Human Error,* 2nd edition, Institution of Chemical Engineers, Rugby, UK, 1991, Chapter 2.
2. *Accident at Markham Colliery, Derbyshire,* Her Majesty's Stationery Office, London, 1974.

3. *Loss Prevention Bulletin,* No. 092, Apr. 1990, p. 9.
4. *Health and Safety at Work,* Vol. 14, No. 12, Dec. 1992, p. 10.
5. J. S. Arendt and D. K. Lorenzo, "Investigation of a Filter Explosion," Paper presented at AIChE Loss Prevention Symposium, San Diego, Aug. 1990.
6. J. A. Senecal, *Journal of Loss Prevention in the Process Industries,* Vol. 4, No. 5, Oct. 1991, p. 332.
7. Health and Safety Executive, *The Fire at Allied Colloids Ltd.*, Her Majesty's Stationery Office, London, 1994.
8. E. H. Frank, private communication.
9. *Operating Experience Weekly Summary,* No. 97-03, Office of Nuclear and Safety Facility, U.S. Dept. of Energy, Washington, D.C., 1997, p.1; No. 97-19, p. 2; No. 97-22, p. 1; and No. 97-30, p 1. See also *Mixing and Storing Incompatible Chemicals,* Safety Note No. 97-1, Office of Nuclear and Safety Facility, U.S. Dept. Of Energy, Washington, D.C., 1997.
10. A. Wilson, *Well Oiled,* Northgate, London, 1979, p. 76.
11. Ministry of Social Affairs and Public Health, *Report Concerning an Inquiry into the Cause of the Explosion on 20th January 1968 at the Premises of Shell Nederland Raffinaderiji NV in Pernis,* State Publishing House, The Hague, The Netherlands, 1968.
12. *Loss Prevention Bulletin,* No. 107, Oct. 1992, p. 24.
13. P. J. Nightingale, *Plant/Operations Progress,* Vol. 8, No. 1, Jan. 1989, p. 28.
14. *Loss Prevention Bulletin,* No. 107, Oct. 1992, p. 24.

Chapter 18

Reverse Flow and Other Unforeseen Deviations

. . . to divide each of the difficulties under examination into as many parts as possible, as might be necessary for its adequate solution.

—René Descartes (1596–1650), *Discourse on Method*

This chapter describes some incidents that occurred because of deviations from the design intention, as expressed in the process flow diagrams (also known as line diagrams or process and instrumentation diagrams). The fact that these deviations could occur was not spotted during the design stage, and they had unfortunate unforeseen results. Ways of spotting these deviations by hazard and operability studies are discussed in Section 18.7.

Errors introduced during modifications are discussed in Chapter 2, while designs that provided opportunities for operators to make errors were discussed in Chapter 3.

One of the most common errors made at the process-flow-diagram stage is failure to foresee that flow may take place in the reverse direction to that intended, as discussed next [1].

18.1 REVERSE FLOW FROM A PRODUCT RECEIVER OR BLOWDOWN LINE BACK INTO THE PLANT

(a) Accidents have occurred because gas flowed from a product receiver into a plant that was shut down and depressured. In one incident

ammonia flowed backward from a storage vessel, through a leaking valve, into a reflux drum, into a still, and out of an open end in the bottoms line, which was open for maintenance (Figure 18-1).

If the possibility of reverse flow had been foreseen, then a slip-plate could have been inserted in the line leading to the ammonia storage vessel, as described in Section 1.1.

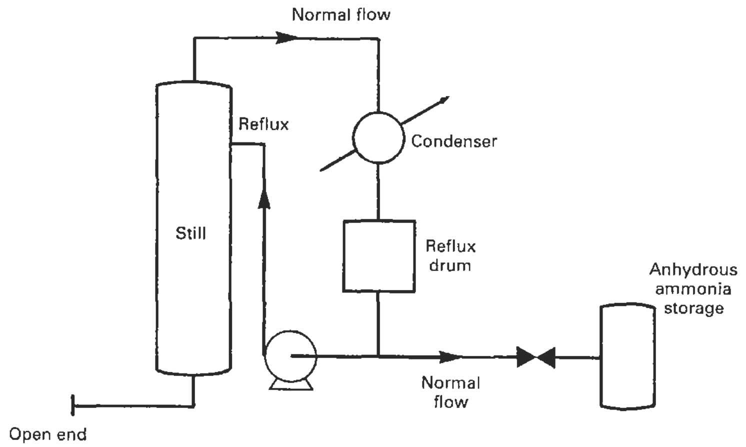


Figure 18-1. Reverse flow occurred from the storage vessel to the open end.

(b) In another incident a toxic gas in a blowdown header flowed through a leaking blowdown valve into a tower and out of the drain valve. The operator who was draining the tower was killed (Figure 18-2).

(c) The contents of a reactor were pumped out into another vessel for further treatment. The pump delivery valve should have closed automatically when the reactor was empty, but on this occasion the automatic system was not working correctly and was on manual control. Fifteen minutes passed before it was closed, and during this time steam traveled backward up the transfer line between the treatment vessel and the reactor and heated a heel of reaction product (about 150 kg), left behind in the reactor, from about 100°C to about 175°C. At this temperature the reaction product, a nitro-compound, decomposed explosively, causing extensive damage [12].

A hazard and operability study was carried out during design, but flow of steam from the treatment vessel to the reactor was never considered as a possible deviation, perhaps because the team

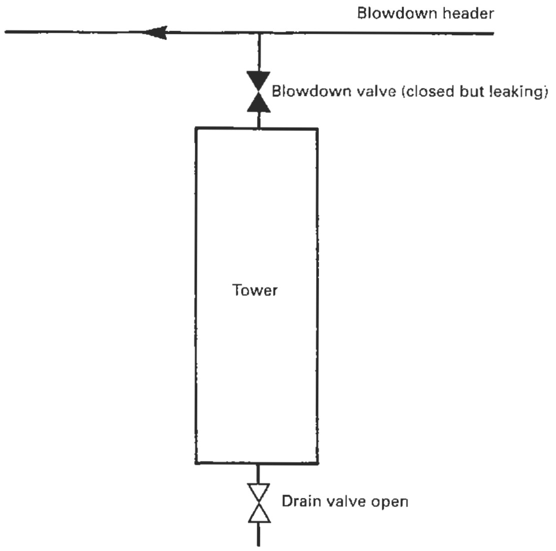


Figure 18-2. Flow occurred from the blowdown header into the vessel and out of the drain valve.

thought that prompt closing of the valve between the two vessels would prevent it. If it had been considered, a check valve might have been inserted in the line. Hazard and operability studies are only as good as the knowledge and experience of the team. In hazard and operability studies, the team members do not always ask what will happen if the automatic equipment is on manual control. This question should always be asked, as safety may depend on the correct operation of such equipment.

(d) Reverse flow into vessels open for entry is discussed in Section 11.3 (e) and (f).

18.2 REVERSE FLOW INTO SERVICE MAINS

This occurs when the pressure in the service line is lower than usual or when the pressure in the process line is higher than usual. Many plants have experienced incidents such as the following:

1. Liquefied gas leaked into a steam line that had been blown down. Ice then formed on the outside of the steam line.
2. A leak on a nitrogen line caught fire.

3. The paint was dissolved in a cabinet that was pressurized with nitrogen; acetone had leaked into the nitrogen [2].
4. A compressed air line was choked with phenol.
5. Toxic fumes in a steam system affected a man who was working on the system (see Section 1.1.4).

Another incident is illustrated in Figure 18-3. Town water should never be directly connected to process lines by a hose [19] or permanent connections. A break tank should be provided.

A service that is used intermittently should be connected to process equipment by a hose, which is disconnected when not in use, or by double block and bleed valves. If a hose is used, it should be provided with a vent so that it can be depressured before it is disconnected.

If a service is used continuously, it may be connected permanently to process lines. If the service pressure is liable to fall below the normal process pressure, then a low-pressure alarm should be provided on the service line. If the process pressure is liable to rise above the normal service pressure, then a high-pressure alarm should be provided on the process side.

In addition, check valves should be fitted on the service lines.

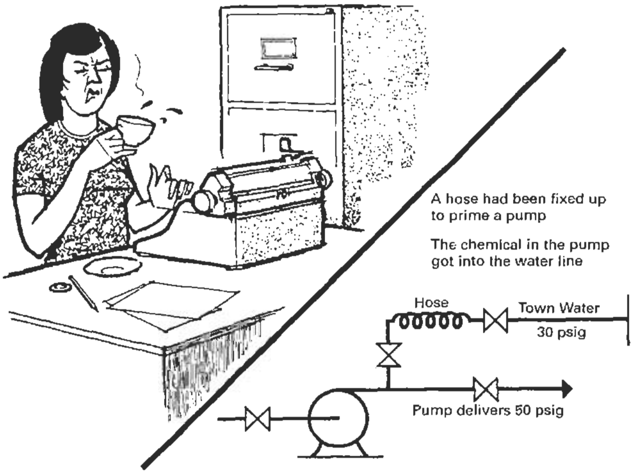


Figure 18-3. Never connect town water to process equipment.

18.3 REVERSE FLOW THROUGH PUMPS

If a pump trips (or is shut down and not isolated), it can be driven backward by the pressure in the delivery line and damaged. Check valves are usually fitted to prevent reverse flow, but they sometimes fail.

When the consequences of reverse flow are serious, then the check valve should be scheduled for regular inspection. The use of two, preferably of different types, in series, should be considered. The use of reverse rotation locks should also be considered.

When lines are being emptied by steaming or by blowing with compressed air or nitrogen, care should be taken that pumps are not turned so fast in reverse (or even forward) that they are damaged.

In one plant, light oil was pumped at intervals from a tank at atmospheric pressure to one at a gauge pressure of 15 psi (1 bar). For many years the practice was not to close any isolation valves but to rely on the check valve in the pump delivery. One day a piece of wire got stuck in the check valve, oil flowed backward, and the atmospheric tank overflowed (Figure 18-4).

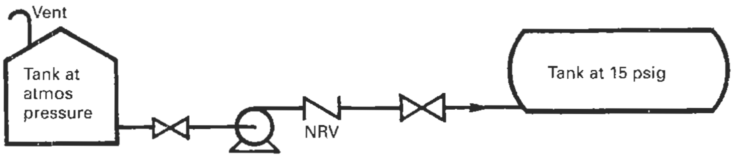


Figure 18-4. The check valve was relied on to prevent backflow, and the isolation valves were not used. A spillage was inevitable.

This is a good example of an accident waiting to happen. Sooner or later the check valve was bound to fail, and a spillage was then inevitable.

In this case the design was not at fault. The operators did not understand the design philosophy. Would this have been foreseen in a hazard and operability study (Section 18.7), and would special attention have been paid to the point in operator training?

18.4 REVERSE FLOW FROM REACTORS

The most serious incidents resulting from reverse flow have occurred when reactant A (Figure 18-5) has passed from the reactor up the reactant B feed line and reacted violently with B.

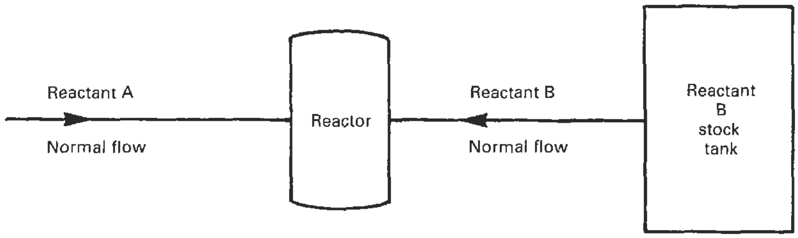


Figure 18-5. Reverse flow of A occurred from the reactor into the B stock tank.

In one incident paraffin wax and chlorine were reacted at atmospheric pressure. Some paraffin traveled from the reactor back up the chlorine line and reacted with liquid chlorine in a catchpot, which exploded with great violence. Bits were found 30 m away [3].

A more serious incident occurred at a plant in which ethylene oxide and aqueous ammonia were reacted to produce ethanolamine. Some ammonia got back into the ethylene oxide storage tank, past several check valves in series and a positive pump. It got past the pump through the relief valve, which discharged into the pump suction line. The ammonia reacted with 30 m^3 of ethylene oxide in the storage tank. There was a violent rupture of the tank, followed by an explosion of the vapor cloud, which caused damage and destruction over a wide area [4].

Another somewhat similar incident occurred when butadiene from a reactor flowed in the wrong direction up a line used for adding emulsifier. The check valve, which should have prevented the flow, was obstructed. The emulsifier tank was in a building and had an open vent. Butadiene came out and exploded. The explosion was heard 15 km away, but damage was minimized by the light construction of the building, which ruptured at the junction of the roof and walls [13].

When such violent reactions can occur, it is not sufficient to rely on check valves. In addition, either:

1. The reactant(s) should be added via a small break tank so that if reverse flow occurs only a small quantity will react and not the main stock, or
2. The pressure drop in the pipeline should be measured, and if it gets too low, a trip valve should be closed automatically. A very reliable, duplicated system may be necessary [16].

A seemingly minor backflow from a reactor occurred on an ammonium nitrate plant, but it led to an explosion. The two reactants, nitric acid and ammonia gas, entered the titanium reactor through separate spargers, and a corresponding amount of ammonium nitrate solution overflowed into a rundown tank. When the plant was shut down for a minor repair, some ammonium nitrate solution flowed backward into the nitric acid sparger and mixed with the acid. Most of it was blown out when the nitric acid line was emptied with compressed air, but a small amount of the ammonium nitrate solution was trapped and left behind. Steam was blown through the acid line to keep the vessel warm. After about nine hours, the sparger exploded, and the explosion spread to the rest of the reactor and the rundown tank. The blast damaged an ammonia tank, and people living within seven miles had to leave their homes. The main recommendations in the report were to redesign the sparger so that liquid could not be trapped in it and avoid the use of titanium, as it increases the sensitivity of ammonium nitrate [17,18].

Reference 14 reviews other ways of preventing backflow.

18.5 REVERSE FLOW FROM DRAINS

This has often caused flammable liquids to turn up in some unexpected places. For example, construction had to be carried out next to a compound of small tanks. Sparks would fall onto the compound. Therefore all flammable liquids were removed from the tanks while the construction took place. Nevertheless a small fire occurred in the compound.

Water was being drained from a tank on another part of the plant. The water flow was too great for the capacity of the drains, so the water backed up into the compound of small tanks, taking some light oil with it. This oil was ignited by welding sparks.

Another incident occurred on a plant that handled liquefied vinyl chloride (VC) (boiling point −14°C). Some of the liquid entered a vessel through a leaking valve, and the operator decided to flush it out to drain with water. As the VC entered the drain it vaporized, and the vapor flowed backward up the drainage system; white clouds came out of various openings. Some of the VC came out inside a laboratory 30 m away, as the pressure was sufficient to overcome the level of liquid in the U-bends. The VC exploded, injuring five people and causing extensive damage. The amount that exploded was estimated as about 35 kg [15].

18.6 OTHER DEVIATIONS

(a) Figure 18-6 shows part of an old unit. Valve A could pass a higher rate than valve B. Inevitably, in the end the lower tank overflowed.

(b) Raw material was fed to a unit from two stock tanks, A and B. A was usually used; B was used infrequently. The raw material was pumped to a head tank from which excess flowed back, as shown in Figure 18-7. The system was in use for several years before the

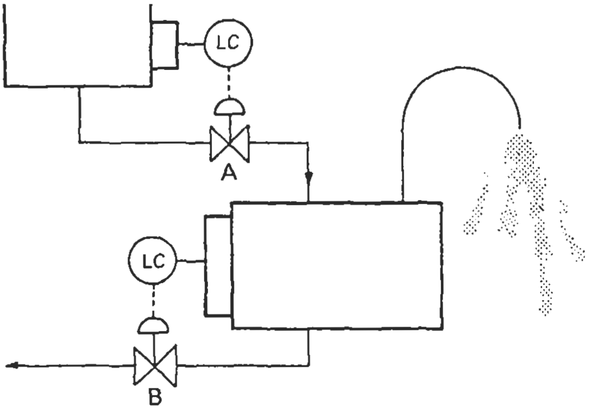


Figure 18-6. Valve A could pass a higher rate than valve B, thus making a spillage inevitable.

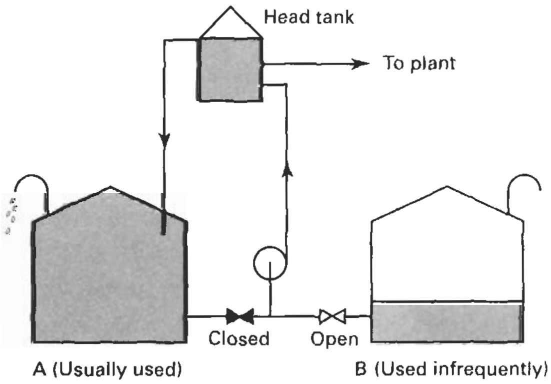


Figure 18-7. If A is full and suction is taken from B, A will overflow.

inevitable happened. Tank B was in use; tank A was full, and the flow from the head tank caused it to overflow.

(c) A funnel was installed below a sample point so that excess liquid was not wasted but returned to the process (Figure 18-8). What will happen if a sample is taken while the vessel is being drained?

The design errors in these cases may seem obvious, but the diagrams have been drawn so that the errors are clear. Originally they were hidden among the detail of a "spaghetti bowl" drawing. To bring the errors to light, it is necessary to go through line diagrams systematically, line by line and deviation by deviation, as described in the next section.

18.7 A METHOD FOR FORESEEING DEVIATIONS

The incidents listed earlier in this chapter and many others could have been foreseen if the design had been subjected to a hazard and operability study (hazop). This technique allows people to let their imaginations go free and think of all possible ways in which hazards or operating problems might arise. But to reduce the chance that something is missed,

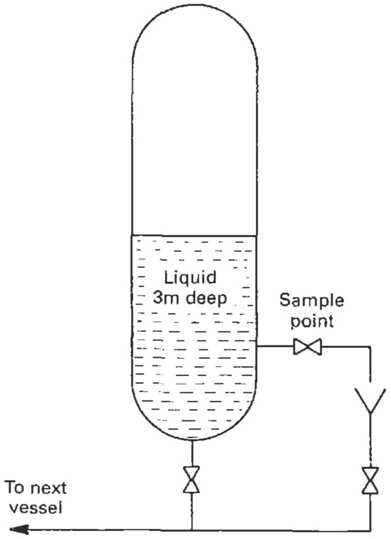


Figure 18-8. What will happen if the vessel is drained while a sample is being taken?

hazop is done in a systematic way, each pipeline and each sort of hazard being considered in turn.

A pipeline for this purpose is one joining two main plant items—for example, we might start with the line leading from the feed tank through the feed pump to the first feed heater. A series of guide words are applied to this line in turn, the words being:

NONE
MORE OF
LESS OF
PART OF
MORE THAN
OTHER

NONE, for example, means no forward flow or reverse flow when there should be forward flow. We ask:

Could there be no flow?

If so, how could it arise?

What are the consequences of no flow?

How will the operators know that there is no flow?

Are the consequences hazardous, or do they prevent efficient operation?

If so, can we prevent no flow (or protect against the consequences) by changing the design or method of operation?

If so, does the size of the hazard or problem justify the extra expense?

The same questions are then applied to "reverse flow," and we then move on to the next guide word, MORE OF. Could there be more flow than design? If so, how could it arise? And so on. The same questions are asked about "more pressure" and "more temperature," and, if they are important, about other parameters, such as "more radioactivity" or "more viscosity."

PART OF prompts the team to ask if the composition of the material in the pipeline could differ from design, MORE THAN prompts them to ask if additional substances or phases could be present, and OTHER THAN reminds them to consider startup, shutdown, maintenance, cata-

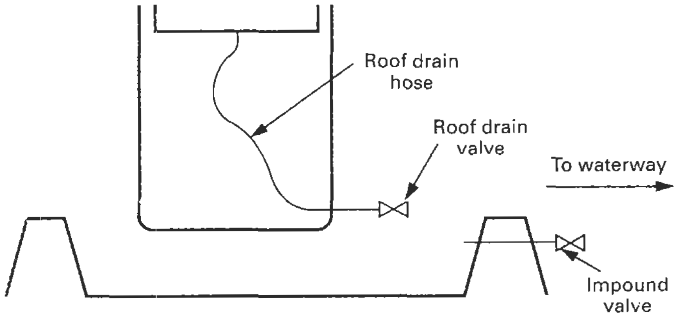
lyst regeneration, services failure, and other abnormal situations. For more detailed accounts of hazop, see References 5 through 10.

18.8 SOME PITFALLS IN HAZOP

The success of a hazop in identifying hazards depends on the knowledge and experience of the team members. If they lack knowledge and experience, the exercise is a waste of time. The following incidents show how an inexperienced team can miss hazards.

(a) Figure 18-9 shows a floating-roof tank located in a dike. Rainwater can be drained from the roof into the dike and from the dike into a waterway. The team members are considering whether any substance other than water can get into the waterway. For this to occur, there would have to be a hole in the hose, and both valves would have to be left open. An inexperienced team may decide that a triple failure is so improbable that there is no need to consider it further. Someone with knowledge of the practicalities of plant operation would realize that during prolonged rain the operators may leave both drain valves open, whatever the instructions say, to avoid frequent visits to the tank. Any hole in the hose will then contaminate the waterway with oil [20].

(b) According to a design, an explosive powder had to be transferred in a scoop. The hazop team realized that this could lead to the for-



(Used with permission from Hydrocarbon Processing, *Apr. 1992. Copyright © 1992 Gulf Publishing Co. All rights reserved.)*

Figure 18-9. Liquid other than rainwater can reach the waterway only if there is a hole in the hose and both valves are left open. This is not as unlikely as it seems at first sight.

mation of an electrostatic charge on the powder and scoop and decided that a metal scoop would be safer than a plastic one. No one realized that if the operator was not grounded, a conducting scoop would increase the risk of ignition, as the charge could pass as a spark from the scoop to ground. A spark from a nonconducting plastic scoop would be less likely to occur and less energetic if it did occur [21]. The best solution is not to use an open scoop.

(c) During the final purification of a product, a small amount of an oxidizing agent had to be added to a much larger amount of hydrocarbon. The reaction between the two substances was known to be highly exothermic and is listed as such in the standard work on the subject, *Bretherick's Handbook of Reactive Chemical Hazards* [22]. However, not one member of the team knew this, and none of them was sufficiently aware to consult this standard work. (Like the men who designed the temporary pipe at Flixborough (Section 2.4 a), they did not know what they did not know.) An explosion occurred after a few months of operation [21].

In all three examples, the senior managers of the companies involved were committed to safety, but the staff lacked the necessary knowledge and experience. It was not necessary for the whole team to have been aware of the hazard. One member's awareness would have been enough, so long as the other team members were willing to listen. It was not necessary for him or her to be fully conversant with the details of the hazard, so long as concerns were followed up.

18.9 HAZOP OF BATCH PLANTS

When studying a batch plant, the guide words should be applied to the instructions as well as the pipelines. For example, if an instruction says that 1 ton of A should be charged to a reactor, the hazop team should consider the effects of the following deviations:

DON'T CHARGE A

CHARGE MORE (OR LESS) A

CHARGE AS WELL AS A

CHARGE PART OF A (if A is a mixture)

CHARGE OTHER THAN A

REVERSE CHARGE A (That is, can flow occur from the reactor to the A storage vessel [see Section 18.4]?)

A IS ADDED EARLY (OR LATE)

A IS ADDED TOO QUICKLY (OR SLOWLY)

Here are three examples of hazards uncovered during hazops of batch processes:

- During the hazop of a batch reaction, when discussing the guide words **AS WELL AS A,** someone asked what contaminants could lead to a runaway reaction. Another member said organic acids could do so. Other members remarked that organic acids were used in another process and were stored in similar drums in the same warehouse. This example shows how hazop is able to combine the knowledge and thoughts of different team members [23].
- During the hazop of another batch process, when discussing services failure, the team members realized that a power failure would result in the loss of both agitation and cooling and that at certain stages of the process this could lead to a runaway reaction. They decided to use town water for emergency cooling and nitrogen injection for emergency agitation [23].
- During the hazop of a proposed experimental rig, it came to light that one of the reactants was hydrogen cyanide, supplied in cylinders, and the designers expected the operators to convey the cylinders to the top floor of the building in the elevator. Toxic or flammable gases and people should never be together in a confined space.
- A large distillation column in a refinery operated at high vapor loads, just above atmospheric pressure. It was not designed for vacuum and so had to be protected if the heat input from the reboiler failed but condensation continued. An inexperienced hazop team might have accepted without comment the original design intention, which was to break the vacuum with fuel gas (or nitrogen if available). A more experienced team might have realized that the volume of gas required was enormous but that it could be reduced to a manageable figure by locating the vacuum breaker valve at the inlet to the condensers, thus blanketing them and reducing heat transfer [24].

18.10 HAZOP OF TANK TRUCKS

Hazop has been applied mainly to fixed plants, but application of the technique to tank trucks used for carrying anhydrous ammonia and liquid carbon dioxide disclosed a number of hazards [11].

18.10.1 More of Pressure

Use of this guide word brought out the fact that if there was a leak on the filling line, there was no way of preventing the contents of the tank truck from flowing backward into the filling line and out to the atmosphere unless the leak was so big that the excess flow valve on the tank truck would operate. This will not occur unless the flow is at least 1½–2 times the normal flow. A remotely operated emergency isolation valve prevents flow from the plant. It was therefore decided to install compressed air cylinders on the tank trucks to operate their internal valves; the cylinders were connected to the plant emergency valve system so that when this was operated, the emergency valves on the tank truck also closed. As a bonus, the internal valves also close if the tanker is driven away while still filling.

The tank trucks were not fitted with relief valves—normal European practice for toxic liquids. The study showed that the plant was designed for a higher pressure than the tank trucks and that in certain circumstances they could be overpressured. Modifications were made.

18.10.2 Less of Temperature

Some of the older tank trucks were made from grades of steel that are brittle at low temperatures, and they are never moved at temperatures below 0°C. It was discovered that some customers wanted liquid carbon dioxide delivered at less than the usual pressure, and arrangements had to be made for them to be supplied only by selected tank trucks. (All new tank trucks are capable of withstanding the lowest temperatures that can be reached.)

18.10.3 More Than

Some customers complained that there was oxygen in the ammonia. It was found that the road transport maintenance department was preparing tanks for repair by washing them out with water and then returning them

to the plant full of air. The oxygen could cause stress corrosion cracking. Arrangements were made for the plant staff to take over responsibility for preparing tank trucks for repair.

REFERENCES

1. T. A. Kletz, *Hydrocarbon Processing,* Vol. 55, No. 3, Mar. 1976, p. 187.
2. T. A. Kletz, *Learning from Accidents,* 2nd edition, Butterworth-Heinemann, Oxford, UK, 1994, Chapter 2.
3. D. B. de Oliveria, *Hydrocarbon Processing,* Vol. 52, No. 3, Mar. 1973, p. 113.
4. J. E. Troyan and R. Y. Le Vine, *Loss Prevention,* Vol. 2, 1968, p. 125.
5. H. G. Lawley, *Chemical Engineering Progress,* Vol. 70, No. 4, Apr. 1974, p. 45.
6. *Hazard and Operability Studies,* Chemical Industries Association, London, 1977.
7. R. E. Knowlton, *An Introduction to Hazard and Operability Studies,* Chemetics International, Vancouver, Canada, 1981, and *A Manual of Hazard and Operability Studies,* Chemetics International, Vancouver, Canada, 1992.
8. T. A. Kletz, *Hazop and Hazan—Identifying and Assessing Process Industry Hazards,* 4th edition, Institution of Chemical Engineers, Rugby, UK, 1999.
9. F. P. Lees, *Loss Prevention in the Process Industries,* 2nd edition, Butterworth-Heinemann, Oxford, UK, 1996, Chapter 8.
10. T. A. Kletz, *Chemical Engineering,* Vol. 92, No. 7, Apr. 1, 1985, p. 48.
11. E. A. George, *Loss Prevention,* Vol. 14, 1981, p. 185.
12. K. Bergroth, *Loss Prevention Bulletin,* No. 109, Feb. 1993, p. 1.
13. F. P. Lees, *Loss Prevention in the Process Industries,* 2nd edition, Butterworth-Heinemann, Oxford, UK, 1996, Appendix B10.
14. S. M. Englund, J. L. Mallory, and D. J. Grinwis, *Chemical Engineering Progress,* Vol. 88, No. 2, Feb. 1992, p. 47.
15. J. Easterbrook and D. V. Gagliardi, *Plant/Operations Progress,* Vol. 3, No. 1, Jan. 1984, p. 29.

16. H. G. Lawley, *Hydrocarbon Processing,* Vol. 55, No. 4, Apr. 1976, p. 247.
17. *Chemical Process Safety Report,* Vol. 5, No. 11, Sept. 1995.
18. *Energetic Events,* Vol. 3, No. 3, Wilfred Baker Engineering, Aug. 1995, p. 4.
19. *Loss Prevention,* No. 124, Aug. 1995, p. 13.
20. D. W. Jones, *Hydrocarbon Processing,* Vol. 71, No. 4, Apr. 1992, p. 78.
21. G. S. Melville, *Journal of Loss Prevention in the Process Industries,* Vol. 7, No. 5, 1994, p. 387.
22. P. G. Urben (editor), *Bretherick's Handbook of Reactive Chemical Hazards,* 5th edition, Butterworth-Heinemann, Oxford, UK, 1995.
23. R. L. Collins, *Chemical Engineering Progress,* Vol. 91, No. 4, Apr. 1995, p. 48.
24. I. M. Duguid, *Loss Prevention Bulletin,* No. 134, Apr. 1997, p. 10.

Chapter 19

I Didn't Know That . . .

This chapter describes some accidents that occurred because people were unaware of accidents that had happened many times before.

19.1 AMMONIA CAN EXPLODE

In reports on ammonia explosions, the authors often say that they were surprised to find that ammonia can explode. For example, a leak of ammonia from the 50-year-old refrigeration system of an ice cream plant in Houston, Texas, ignited and severely damaged the building. The ignition source was not identified, but there were several possible sources. The chief of the Houston Fire Department Hazardous Materials Response Team wrote, "The hazards, it was believed, were limited to health; never had much thought been given to the flammability of ammonia" and "It is hard to find any of the old, experienced ammonia refrigeration men who believe it possible for ammonia to explode" [1].

Another explosion occurred in Brazil. Welding had to be carried out on the roof of an aqueous ammonia tank. The tank was emptied but not gas-freed. When a welder applied his torch to the roof, the tank blew up. The welder survived but was crippled for life.

Ammonia explosions are not common, as the lower explosive limit (LEL) of ammonia is unusually high: 16%; the upper limit is 25%. Typical limits for hydrocarbons are propane, 2–9.5%, and cyclohexane, 1.3–8.3%. In addition, the auto-ignition temperature of ammonia is high, about 650°C, compared with about 480°C for propane and about 270°C for cyclohexane, so ammonia is harder to ignite. Nevertheless, there was little excuse for the ignorance of the responsible people in Texas and

Brazil, as ammonia explosions have occurred from time to time and the explosibility of ammonia has been known since at least 1914 [2]. In a paper presented in Houston in 1979, Baldock said that a number of ammonia leaks had exploded although some reported incidents may not have been due to ammonia at all. He gave no details. He added that there had been 11 explosions in aqueous ammonia tanks and several explosions in nitric acid plants when the ammonia/air ratio became too high [3].

A series of incidents in one nitric acid plant has been described in detail [21]. Rust passed through the ammonia gas filter and catalyzed oxidation of the ammonia in the ammonia/air mixer and in the pipe leading from it to the platinum catalyst. This occurred even though the ammonia concentration was below the normal flammable limit. The temperature of the pipe rose from 220°C to more than 1000°C in an hour, and then the pipe ruptured. This damaged the platinum catalyst, and some dust from it ended up in the ammonia/air mixer. As a result several further ignitions occurred after the plant was repaired and restarted. On these occasions it was shut down at once, before the pipework failed. The report admits that the mixer had not been cleaned for years as "it was so time consuming to remove it." (Compare the tank that was sucked in because the flame arrestors had not been cleaned for two years [Section 5.3 a].) The report recommended installation of high-temperature alarms as well as regular cleaning of the mixer.

In 1968, an explosion in a sausage plant in Chicago killed 9 people, including 4 firemen, injured 72, and destroyed the plant. The incident started when a gasoline tank truck hit an obstruction. The gasoline leaked into a basement and caught fire. The fire heated a 300-lb (136-kg) ammonia cylinder, which discharged its contents through the relief device. The ammonia rose into the ground floor area and the floor above where it exploded. It was assumed that, because of its high LEL, the ammonia was able to pass through the fire zone without igniting and then accumulate in a confined space until the concentration reached 16%.

Brief reports have appeared of several other ammonia fires or explosions:

- An explosion occurred in 1976 while a refrigeration plant in Hexham, England, was being demolished [4].
- A fire broke out in 1977 at Llandarcy, South Wales, fed by leaking ammonia valves [5].

- A fire and explosion occurred in 1978 in a disused cold store in Southwark, London [6].
- In Enid, Okla., in 1978, the refrigeration system on an ammonia storage vessel failed. The ammonia warmed up, its pressure rose, and some ammonia was discharged through a relief valve and ignited by a nearby flare [14].
- A welder was killed by an explosion in New Zealand in 1991 while working on an empty 28-m^3 tank, which contained a flammable mixture of ammonia vapor and air.

A feature of ammonia explosions is that any ammonia that continues to leak out after the explosion may not burn, as its concentration may be too low.

So far as I am aware, ammonia has never exploded in the open air, and it is doubtful if a concentration as high as 16% could be attained out-of-doors. In 1989, at Jovona, Lithuania, a storage tank split from top to bottom, and 7,000 tons of liquid ammonia were spilled. The pool caught fire [15, 16], but according to later reports, the fire was due to rupture of a natural gas line that passed through the area [17].

What can we do to prevent ammonia explosions? The action required is much the same as for other flammable gases, namely:

1. Use equipment of sound design and construction. (The Houston ice cream plant was not up to today's standards but had been "grandfathered.")
2. Use nonflammable refrigerants instead of ammonia.
3. If ammonia is used, see that the ventilation is adequate. (It does not have to be all that good to prevent the ammonia concentration from reaching 16% but has to be reasonably good if we wish to prevent the ammonia concentration from reaching 10,000 ppm, the concentration that is fatal to about 50% of people in 30 minutes.)
4. Gas-free and test before introducing a source of ignition.

19.2 HYDRAULIC PRESSURE TESTS CAN BE HAZARDOUS

As water is incompressible, hydraulic pressure tests are often considered safe. If the vessel fails, the bits will not fly very far.

Hydraulic pressure testing is safer than pneumatic testing, as much less energy is released if the equipment fails. Nevertheless, some spectacular failures have occurred during hydraulic tests. In 1965 a large pressure vessel (16 m long by 1.7 m diameter), designed for operation at a gauge pressure of 350 bar, failed during pressure test at the manufacturer. The failure, which was of the brittle type, occurred at a gauge pressure of 345 bar, and four large pieces were flung from the vessel. One piece weighing 2 tons went through the workshop wall and traveled nearly 50 m. Fortunately, there was only one minor injury. The failure occurred during the winter, and the report recommends that pressure tests should be carried out above the ductile-brittle transition temperature for the grade of steel used. It also states that the vessel was stress-relieved at too low a temperature [7]. Another similar failure is described in Reference 8. Substandard repairs and modifications were contributory factors.

When carrying out pressure tests, remember that the equipment may fail, and take precautions accordingly. If we were sure that the equipment would not fail, we would not need to test it (see Section 14.8). Reference 22 gives advice on the measures necessary. Remember also that equipment may fail during on-line pressurization with process materials if the temperature is too low [8]. I do not know of any vessels that have burst for this reason, but rupture discs have failed because they were too cold.

19.3 DIESEL ENGINES CAN IGNITE LEAKS

Most companies do not allow spark ignition (gasoline) engines to enter areas where flammable gases or liquids are handled, except under very strict control, as a leak of gas or vapor might be ignited by the spark mechanism. Many companies, however, allow uncontrolled access by diesel engines, believing that they cannot ignite gas or vapor. This is incorrect, as the following incident shows.

Four tons of hot, flammable hydrocarbon leaked out of a plant while maintenance work was in progress. A diesel engine was operating in the area. The hydrocarbon vapor was sucked into the air inlet, and the engine started to race. The driver tried to stop it by isolating the fuel supply, the usual way of stopping a diesel engine, but without success, as the fuel was reaching the engine through the air inlet. Finally flashback occurred, and the hydrocarbon was ignited. Two men were killed [9].

Another incident occurred when a tank truck drove underneath a loading arm that was dripping gasoline. The engine started to race and emitted black smoke, but fortunately no ignition occurred [10].

In yet another incident a hydraulic hose leaked, and an oil mist was sucked into the air inlet of a diesel engine. It continued to run for three to five minutes after the normal fuel supply was isolated. The air filter on the engine was missing. Had it been present, it would probably have trapped the oil mist [23].

Proprietary devices that shut off the air supply as well as the fuel supply are available for protecting diesel engines that have to operate in areas in which leaks of flammable gas or vapor may occur [11]. However, diesel engines can ignite leaks of flammable gas or vapor in other ways. Sparks or flames can be emitted by the exhaust, the exhaust pipe can be hot enough to ignite the vapor directly [23], and ancillary equipment, such as electrical equipment, can produce sparks. One explosion occurred because an engine was stopped by use of the decompression control. Spark arrestors and flame arrestors should therefore be fitted to the exhaust, its temperature should be below the auto-ignition temperature of the materials handled, electrical equipment should be protected, and if a decompression control is fitted it should be disconnected.

The degree of protection adopted in any particular case will depend on the length of time the diesel engine is present and the degree of supervision [12]. A truck delivering goods does not need any special protection but should not be allowed to enter the plant area unless conditions are steady and leaks unlikely. Plants should be laid out so that such vehicles do not normally have to enter areas where flammable gases or liquids are handled. A diesel pump that is permanently installed or a tow motor (forklift truck) in everyday use requires the full treatment. An intermediate level of protection is suitable for a crane or pump used occasionally. It should be fitted with a device for shutting off the air supply, and it should never be left unattended with the engine running. Pumps driven by compressed air are safer than diesel pumps. Flooded drains and sumps can be emptied with ejectors powered by a water supply.

An entirely different diesel hazard is compression of a pocket of air and flammable vapor trapped in a vessel or pipeline by a column of liquid. If the pressure of the liquid rises, the air is compressed, and the heat developed may heat the vapor above its auto-ignition temperature [13].

19.4 CARBON DIOXIDE CAN IGNITE A FLAMMABLE MIXTURE

In 1966, a naphtha tanker, the *Alva Cape,* was involved in a collision near New York and was severely damaged. Some naphtha was spilled, and the rest was pumped out into another vessel. The owners wanted to move the ship to a shipyard where it could be gas-freed and the damage could be surveyed, but the New York Fire Department said that the ship's tanks should be inerted before it was moved. The salvage company, therefore, ordered some carbon dioxide cylinders and hoses. Two tanks were inerted without incident, but when carbon dioxide was discharged into a third tank, an explosion occurred, followed by a fire. Four men were killed, and further explosions occurred in other tanks when they were heated by the fire.

When the carbon dioxide was discharged, the adiabatic cooling caused particles of solid carbon dioxide to form, and these collected a charge of static electricity (see Section 15.2). The charge discharged as a spark and ignited the mixture of naphtha vapor and air in the tank. The company that supplied the carbon dioxide did not know how it would be used but warned the salvage company that it was hazardous to inert tanks with carbon dioxide. The vessel was towed out to sea and sunk by gunfire [18].

A similar incident occurred in France a year or two later. Carbon dioxide was injected into a tank containing jet fuel during a tryout of a fire-fighting system. The tank exploded, killing 18 people who were standing on the top.

19.5 MISTS CAN EXPLODE

Most everyone knows that dusts—fine particles of solid—can explode, but not everyone is aware that mists—fine droplets of liquid—can explode just as easily and that they can explode at temperatures far below the flash point of the bulk liquid or vapor [19].

For example, a material had been oxidized many times without incident in 1- and 4-L vessels, in an oxygen atmosphere, at a temperature of 80°C, and at a gauge pressure of 225 psi (15.5 bar). The flash point of the solvent at this temperature and pressure was 130°C. The next step was to scale up to a 48-L vessel. The rate of reaction was limited by the rate at

which the oxygen and the material to be oxidized could be brought into contact, so a highly efficient gas-dispersing and agitation system was installed. This filled the vapor space of the reaction vessel with a fine mist, and several hours after startup, the vessel exploded. The pressure or temperature did not rise beforehand, so the explosion could not have been due to a runaway reaction; it was a mist explosion. The source of ignition was a small amount of a catalyst left over from an earlier set of experiments [20].

The introduction of the efficient agitation system was a process modification (see Section 2.6), but its consequences were not foreseen.

Another incident occurred when contractors were employed to clean several black oil tanks, 4,500-m^3 capacity, so they could be used for the storage of kerosene. The details of the contract were agreed verbally. After removing solid residues and the heater coils, the tanks would be sprayed with hot water and a detergent. Floodlights were suspended through roof manholes and were to be removed before the tanks were sprayed.

The first tank was cleaned without incident. By the time the contractors started on the second tank, a new foreman was in charge. To soften the deposits, he disconnected the steam coil, blew live steam into the tank, and then sprayed kerosene onto the walls, section by section, using a spinner mounted on a tripod. The report does not make it clear whether or not the kerosene was heated. While men were moving the tripod, a fire started in the tank, followed by an explosion. Three men were killed, one by the fire and two by falling bits of the external concrete cladding.

Survivors said that conditions in the tank resembled a thick fog, and this was confirmed by tests. The source of ignition was either the floodlights, which had been left in position and had a surface temperature of 300°C, or a discharge of static electricity generated by the steam cloud. Tests showed that the oil mist could ignite at 11°C, 60°C below the flash point of the oil. Though not suggested in the report, the hot steam pipe could also have been a source of ignition. The contractors were fined. It seems that they had no idea that mists could explode, or if they did know, they failed to tell their foreman [24].

Oil mist explosions have often occurred in the crankcases of reciprocating engines. They can be prevented by installing relief valves.

The incidents described in Sections 12.4.5 and 17.12 were also mist explosions.

19.6 THE SOURCE OF THE PROBLEM LAY ELSEWHERE

The cause of a problem may be difficult to find when it lies in another part of the plant. One example was described in Section 2.6 (a). Here are two more.

The product from a new plant was purified in a vacuum distillation column. Soon after startup the column developed a high-pressure drop. It was opened up for inspection, and the lower trays were found so full of solid that the pressure drop had caused them to buckle. Analysis showed that the solid was a polymer of the product; traces of the reaction catalyst were present and had presumably caused the polymerization. The obvious solution was to remove the traces of catalyst before distillation; this would have been expensive, so changing the operating conditions was tried first. Lower throughput was tried, then lower boil-up. Next on the list was a lower pressure, which would give lower temperatures. It proved impossible to lower the pressure, though the vacuum system should have been able to pull a harder vacuum. Was there a leak of air into the plant? A pressure test showed that there was, in the seal of the bottoms pump. When this was repaired the polymerization problem disappeared. Oxygen as well as traces of catalyst were needed for polymerization. The pump seal was padded with nitrogen so that if it leaked again only nitrogen would enter the column.

A reactor was cooled by a molten salt. At startup the salt was heated to reaction temperature by an electric heater. During one startup the temperature of the salt rose at only half the usual rate. Obviously one of the heaters was faulty, but no fault could be found. The problem was finally traced to a nitrogen valve, which had been left open. The flow of nitrogen through the reactor was taking away half the heat.

Commenting on these two incidents, Gans *et al.* say that big failures usually have simple causes while marginal failures usually have complex causes. If the product bears no resemblance to design, look for something simple, like a leak of water into the plant. If the product is slightly below specification, the cause may be hard to find. Look for something that has changed, even if there is no obvious connection between the change and the fault [25].

REFERENCES

1. M. H. McRae, *Plant/Operations Progress,* Vol. 6, No. 1, Jan. 1987, p. 17.
2. Reis, *Zeitschrift Physikal. Chem.*, Vol. 88, 1914, p. 513.
3. P. J. Baldock, *Loss Prevention,* Vol. 13, 1980, p. 35.
4. *Northern Echo,* Darlington, UK, May 15, 1976.
5. *Lloyds List,* London, June 20, 1977.
6. *Lloyds List* and *The Times,* London, Jan. 11, 1978.
7. *British Welding Research Association Bulletin,* Vol. 7, Part 6, June 1966, p. 149.
8. P. G. Snyder, "Brittle Fracture of a High Pressure Heat Exchanger," Paper presented at AIChE Loss Prevention Symposium, Minneapolis, Aug. 1987.
9. *Chemical Age,* Dec. 12, 1969, p. 40; and Jan. 9, 1970, p. 11.
10. *Petroleum Review,* Apr. 1984, p. 36.
11. *Hazardous Cargo Bulletin,* Jan. 1983, pp. 22, 24.
12. Oil Companies Materials Association, *Recommendations for the Protection of Diesel Engines Operating in Hazardous Areas,* Wiley, Chichester, UK, 1977.
13. O. A. Pipkin, in C. H. Vervalin (editor), *Fire Protection Manual for Hydrocarbon Processing Plants,* Vol. 1, 3rd edition, Gulf Publishing Co., Houston, Texas, 1985, p. 95.
14. M. Kneale, "The Safe Disposal of Relief Discharges," *Selection & Use of Pressure Relief Systems for Process Plants,* Institution of Chemical Engineers North Western Branch, Manchester, UK, 1989, Paper 7.
15. B. O. Andersson, "Lithuania Ammonia Accident," *Hazards XI—New Directions in Process Safety,* Symposium Series No. 124, Institution of Chemical Engineers, Rugby, UK, 1991.
16. B. O. Andersson and J. Lindley, *Loss Prevention Bulletin,* No. 107, Oct. 1992, p. 11.
17. T. A. Kletz, *Journal of Loss Prevention in the Process Industries,* Vol. 5, No. 4, 1992, p. 255.

18. *Fire Journal,* Nov. 1967, p. 89.
19. J. Eichhorn, *Petroleum Refiner,* Vol. 34, No. 11, Nov. 1955, p. 194.
20. H. T. Kohlbrand, "Case History of a Deflagration Involving an Organic Solvent/Oxygen System Below its Flash Point," Paper presented at AIChE Loss Prevention Symposium, San Diego, Aug. 1990.
21. W. D. Verduijn, *Plant/Operations Progress,* Vol. 15, No. 2, Summer 1996, p. 89.
22. G. Saville, B. Skillerne de Bristowe, and S. M. Richardson, "Safety in Pressure Testing," *Hazards XIII—Process Safety: The Future,* Symposium Series No. 141, Institution of Chemical Engineers, Rugby, UK, 1997.
23. *Loss Prevention Bulletin,* No. 133, Feb. 1997, p. 17.
24. Health and Safety Executive, *Report on Manufacturing and Service Industries 1982,* Her Majesty's Stationery Office, London, 1983, p. 13.
25. M. Gans, D. Kohan, and B. Palmer, *Chemical Engineering Progress,* Vol. 87, No. 4, Apr. 1992, p. 25.

Chapter 20

Problems with Computer Control

The use of computers and microprocessors (also known as programmable electronic systems [PES]) in process control continues to grow. They have brought about many improvements but have also been responsible for some failures. If we can learn from these failures, we may be able to prevent them from happening again. A number of them are therefore described below. Although PES is the most precise description of the equipment used, I refer to it as a computer, as this is the term usually used by the nonexpert.

20.1 HARDWARE AND SOFTWARE FAULTS

Most hardware faults occur in the measurement and control systems attached to the computer rather than in the computer hardware itself, but computer faults do occur and are more common than was once thought. Their effects can be reduced by installing "watchdogs," devices that detect computer failures. However, one accident in which valves were opened at the wrong time and several tons of hot liquid were spilled was due to an error in a watchdog card [1]. Some incidents have been due to voltage variations, including those caused by lightning [2], which in one case caused a computer to leave out a step in a sequence. Systems should be designed so that the effects of foreseeable failures of power or equipment are minimized, and hazard and operability studies (see Section 18.7) should include a check that this has been done.

Software faults can occur in the systems software that comes with the computer or in the applications software written for the particular application. Systems software faults can be reduced by using only well-tested systems—not always easy in a rapidly changing field. Applications software faults can be reduced by thorough testing to make sure that the program behaves as we want it to during abnormal as well as normal conditions. Such testing can take longer than design, and even then some faults may be missed and may lie like time bombs, waiting for a particular combination of unusual conditions to set them off. It is impossible to test every possible pathway in a computer system.

The view is therefore growing that we should try to design plants so that they are safe even if there is a fault in the software. This can be done by adding on independent safety systems, such as relief valves and hard-wired trips and interlocks, or by designing inherently safer plants that remove the hazards instead of controlling them (see Chapter 21).

There is an important difference in the failure modes of hardware and software. Computer hardware is similar to other hardware. Once initial faults have been removed and before wear becomes significant, failure can be considered random and treated probabilistically. In contrast, failure of software is systemic. Once a fault is present, it will always produce the same result when the right conditions arise, wherever and whenever that piece of software is used. There is no agreed method for estimating the type and number of faults that might occur, and it is impossible to be 100% confident that we have found them all by testing. For this reason many people, including some authorities, are reluctant to use a computer for the last line of protection on a high-hazard plant. If a computer is used, it should be independent of the control computer.

Errors in written instructions are also systemic, but it is easy for the author to check them, and readers can understand what is meant even though they contain errors in spelling or grammar or are ambiguous. We know what is meant if we are told to save soap and waste paper.

20.2 TREATING THE COMPUTER AS A BLACK BOX

The most common types of errors are probably those that occur because operators treat the computer as a "black box," that is, something that will do what we want it to do without the need to understand what goes on inside it. There is no fault in the hardware or software, but nevertheless the system does not perform in the way that the designer or oper-

ators expected it to perform. The fault is in the specification and arises because the software engineer did not understand the designer's or operator's requirements or was not given sufficiently detailed instructions covering all eventualities. Operators can do what we want them to do even though we have not covered the point precisely; they can decode vague instructions. A computer, however, can do only what it is told to do.

Errors of this type can be reduced by carrying out hazard and operability studies, or hazops (see Section 18.7), on the instructions given to the computer as well as on the process lines. We should ask what the computer will do for all possible deviations (no flow, reverse flow, more flow, more pressure, more temperature, etc.), for all operating modes, and for all stages of a batch process. The software engineer should be a member of the hazop team. This will give him or her a better understanding of the process requirements and will give the process engineers and the people who will operate the plant a better understanding of the capabilities of the control system.

20.2.1 The Hazards of Complexity

A pump and various pipelines were used for three different duties: for transferring methanol from a tank truck to storage, for charging it to the plant, and for moving recovered methanol back from the plant (Figure 20-1). A computer set the various valves and monitored their positions.

A tank truck was emptied. The pump had been started from the control room but had been stopped by means of a local button. The next job was to transfer some methanol from storage to the plant. The computer set the valves, but as the pump had been stopped manually, it had to be started manually. When the transfer was complete, the computer told the pump to stop; but as it had been started manually, it did not stop, and a spillage occurred [3].

A thorough hazop probably would have revealed that this error could have occurred. The control system could have been modified, or better still, separate lines could have been installed for the various different movements, thus greatly reducing the opportunities for error. The incident shows how easily errors in complex systems can be overlooked if the system is not thoroughly analyzed. In addition, it illustrates the paradox that we are very willing to spend money on complexity but are less willing to spend it on simplicity [4]. Yet the simpler solution, indepen-

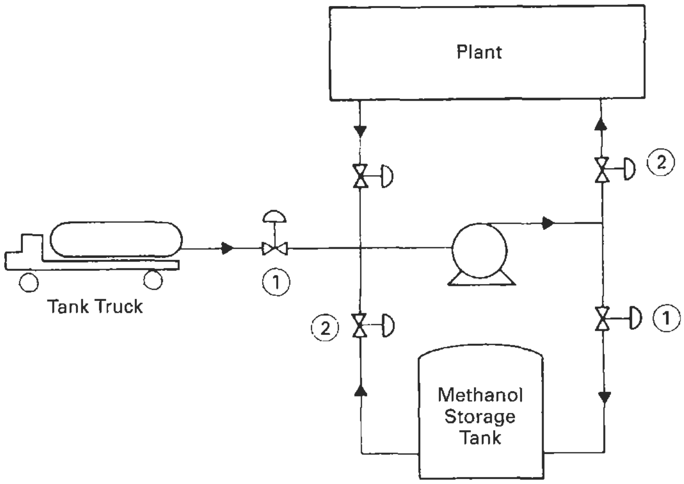


Figure 20-1. A pump and lines, controlled by a computer, were used for several different jobs. The pump could also be started and stopped locally. (1) Valves open for first job; others closed. (2) Valves open for second job; others closed.

dent lines (actually installed after the spillage), makes errors much less likely and may not be more expensive if lifetime costs are considered. Control systems need regular testing and maintenance, which roughly doubles their lifetime cost (even after discounting), while extra pipelines involve little extra operating cost.

20.2.2 Unforeseen Effects of a Small Leak

A pressure filter was controlled by a computer. It circulated the liquor through the filter for two hours. As more solid was deposited on the filter, the pressure drop increased. To measure the pressure drop, the computer counted the number of times that the pressure of the air in the filter needed to be topped up in 15 minutes. It had been told that if less than five top-ups were needed, filtration was complete, and it could move on to the next phase: smoothing the filter cake. If more than five top-ups were needed, the liquor was circulated for a further two hours.

There was a leak of compressed air into the filter, which misled the computer into calculating that filtration was complete. The computer signaled completion to the operator, who opened the filter door; the entire batch—liquid and solid—was spilled.

To be fair to the computer, or rather to the programmer, the computer had detected that something was wrong—there was no increase in power consumption during smoothing—and had signaled this finding by stopping the operation, but the operator ignored this warning sign or did not appreciate its significance [3].

Again, a hazop would probably have disclosed the weakness in the system for detecting the pressure drop through the cake, and changes could have been made. In particular, the filter should have been fitted with a device to prevent the operator from opening it more than a crack while it was full of liquid. Many accidents have occurred because operators opened up autoclaves or other pressure vessels while they were up to pressure (see Sections 13.5 and 17.1). Opening up a vessel while it is full of liquid is not as dangerous but, nevertheless, dangerous enough.

20.2.3 Unforeseen Effects of a Measurement Failure

The furnace on a steel plant was started up from cold shutdown after repair. The temperature indicator was out of order and continually registered a low temperature. The computer, therefore, supplied the maximum fuel-gas rate to the furnace and continued to supply it after an hour, when the furnace was hot. After four hours the furnace was seriously damaged [5].

Instrument failure is a foreseeable event and should be considered during design by means of a hazard and operability study, a failure mode and effect analysis (FMEA), or some other way. One wonders what the operators were doing. Did they have such confidence in the computer that they never bothered to look at the information displays? If the furnace had not been controlled by a computer, even the most inept operator would have suspected that something was wrong if the temperature had not changed after an hour. The computer, of course, could have been programmed to sound an alarm if the temperature did not change after a period of time, but no one recognized the need to tell it to do so. A hazop or FMEA could have shown the need.

This illustrates a point that applies to all the incidents described in this chapter: computers do not introduce new errors, but they can provide new opportunities for making old errors; they allow us to make more errors faster than ever before. Incidents will occur on any plant if we do not check readings from time to time or if instructions do not allow for foreseeable failures of equipment.

20.2.4 Changing Trends May Not Be Noticed

This incident occurred on a plant where the possibility of a leak of liquid had been foreseen; a sump had been provided into which any leaks would drain, and a level alarm would then sound. Unfortunately, when a leak occurred, it fell onto a hot surface; most of it evaporated, leaving a solid residue. Because no liquid entered the sump, the leak was not detected for several hours.

The operators could have detected that something was wrong by a careful comparison of trends in a number of measurements, but they saw no need to make such a comparison, as they were not aware of any problem. They did not normally display the relevant measurements on the computer screens and had not called them up. Afterward, the operators said the spillage would have been detected earlier if the chart recorders had not been removed from the control room when the computer was installed in place of the original control equipment.

The computer could have been programmed to carry out mass balances, compare readings for consistency, and/or sound an alarm (or, better, display a message advising the operators that something was amiss) when unexpected measurements were received, but no one had foreseen the need to program it so. It is also possible to install additional screens that can continuously display the trends of selected measurements, in much the same way as old-fashioned chart recorders did. It is, however, easier to change the scale or the measurements displayed. (Though not relevant to this case, a computer can also detect the absence of noise in measuring instruments that are "stuck.") [6].

20.2.5 An Error That Would Not Be Made Without a Computer

A computer was controlling a batch reaction on a chemical plant during the night, when daylight saving time ended, and the clocks had to be put back one hour. The operator reset the computer's clock so that it indicated 2 a.m. instead of 3 a.m. The computer then shut the plant down for an hour until the clock indicated 3 a.m. again [7]. Perhaps hazard and operability studies should consider reverse flow of time as well as reverse flow of liquids!

20.3 MISJUDGING THE WAY OPERATORS WILL RESPOND

This comes close to the last category as a source of error, and there is much scope for improving the operator/computer interface. The following are some of the incidents that have occurred:

(a) When a power failure occurred, the computer printed a long list of alarms. The operator did not know what had caused the upset, and he did nothing. After a few minutes an explosion occurred. Afterward, the designer admitted that he had overloaded the operator with too much information but asked the operator why he did not assume the worst and trip the plant. Unfortunately, when people are overloaded by too much information, they tend to switch off (themselves, not the computer) and do nothing. Computers make it easy to overload people with too much information.

(b) The information that operators need for dealing with an alarm is often distributed between several pages of the display. It should be possible to bring together on a special page for each major alarm the information needed for dealing with it [8].

Different display pages often look alike, which saves development time and costs. But during an emergency, an operator may turn to the wrong page and not realize immediately that he has done so.

(c) To reduce the chance that operators will enter the wrong data or instructions, computers are often programmed so that when the Enter button is pressed, the data or instructions are displayed for the operator to check, and then the Enter button has to be pressed again. Unfortunately, operators soon get into the habit of pressing the Enter button twice in rapid succession after entering data or instructions. It is better if operators have to carry out two distinct operations after entering data, for example, moving a cursor before pressing Enter the second time.

(d) A computer was taken off line so that the program could be changed. At the time, it was counting the revolutions on a metering pump, which was feeding a batch reactor. When the computer was put back on line, it continued counting where it had left off, and the reactor was overcharged.

(e) A computer collected spot values of each instrument reading every minute and then wrote them onto a hard disk every five minutes. The hard disk survived a runaway reaction followed by an explosion, but the explosion occurred toward the end of one of the five-minute periods, and all the data for the five minutes immediately before the explosion was lost. The highest pressure recorded was 60 psi (4 bar), although the bursting pressure of the ruptured reactor was about 900 psi (60 bar) [9].

(f) Some operators seem to expect computers to behave like humans and cannot understand why they make mistakes no human would make. These people instinctively trust seemingly intelligent machines. According to one report, even when alarms were sounding, the operator did not believe it was a real emergency; "the computer can cope," he believed [13].

20.4 OTHER PROBLEMS

20.4.1 Errors in the Data Entered in the Computer

An operator wanted to reduce the temperature on a catalytic cracker from 982°F to 980°F. Unfortunately, he pressed the keys in the wrong order (908) and immediately pressed the Enter key. The computer responded with impressive speed, slamming slide valves shut and causing a flow reversal along the riser. Fortunately, there were no injuries and only a small fire at a leaking joint.

Standards should be written and vendors should be chosen so that the computer will reject or query data or instructions that are outside specified ranges, that deviate more than a specified amount from the existing value, or that fail consistency tests.

On another occasion, an operator was changing a feed rate from 75 to 100 gal per minute. She entered 1,000 in error. The computer opened the feed valve to the full extent, raising the pressure in the plant. There was no damage, however, because the relief valve lifted [10]. A second line of defense, as recommended at the end of Section 20.1, countered an error in the design of the software—failure to foresee and allow for a slip that operators can easily make.

It is possible for errors to occur because data are entered in the wrong units. I do not know of any incidents in the process industries where this

has occurred, but a plane became short of fuel and had to make a forced landing because x lbs of fuel were loaded instead of x kg.

20.4.2 Failures to Tell Operators of Changes

I do not know of any incidents in the process industries that have occurred because operators were not told of changes in data or programs, but this has caused an aircraft accident. In 1979, the destination waypoint of an Air New Zealand sightseeing flight to Antarctica was moved 2° to the east, but the crew members were not told. The inertial navigation system guided the plane, which was flying low so the passengers could see the scenery, along a valley that ended in a cliff. It looked very similar to the open-ended valley that the crew memers expected to follow. They did not realize they were on the wrong course, and they flew into the cliffs. All 257 people on board were killed [11, 12].

20.4.3 Modifications

Chapter 2 stressed the need to consider the results of plant modifications before they are made and to prevent unauthorized ones. This applies to computers as well as traditional plant. No change should be made to hardware or software unless authorized by a professionally competent person who has carried out a systematic survey of possible consequences. It is easier to change a software control system than a traditional one and therefore harder to control the changes, but it is just as important to do so. Section 20.5 describes an unauthorized change to hardware that could have had serious results.

20.4.4 Old Software

Sections 9.1.6 (c) and 9.2.1 (h) drew attention to the hazards of using old equipment. Similar remarks apply to old software except that, unfortunately, it never wears out. I do not know of any incidents in the process industries due to this cause, but it was responsible for the loss of the European space rocket *Ariane 5*. A function that no longer served any purpose was left in "for commonality reasons," and the decision to do so "was not analyzed or fully understood" [14]. In another incident, cancer patients received excessive doses of radiation because operators were able to enter data faster than the computer could process them. This had always been the case, but originally a hardwired interlock had prevented

the excessive dose. The interlock was removed when the old software was "improved" [15,16].

20.5 UNAUTHORIZED INTERFERENCE

Unauthorized interference with computer hardware is usually difficult, but interference with peripheral equipment may be more serious than on a traditional plant, as the computer will not know that interference has occurred. For example, the leads on a limit switch on a valve were interchanged to carry out some tests. The plant was on manual control at the time but was switched back to computer control before the leads were restored to their correct positions. The computer "thought" the valve was open (when it was shut) and elected to close it. It actually opened it, releasing flammable material [2].

If the plant had been controlled conventionally, the operators involved may have known of the temporary interchange of the leads, or a notice could have been placed on the panel informing them. However, it would be difficult to tell the computer that the valve is open when the signal says it is shut! A computer provides new opportunities for familiar communication errors.

Files had to be transferred from a control computer to a training simulator. At first, there was no direct connection; the files were first transferred to a freestanding workstation and then from there to the simulator. To simplify the transfer, a direct cable connection was made between the control computer and the simulator.

Unfortunately the address of the gateway in the control computer used for the data transfer was the same as that used to connect to the distributed control system (dcs). As a result data flowed from the simulator through the control computer to the dcs and replaced the current input data by historic data. Some conditions on the plant started to change, but fortunately this was soon noticed by alert operators, and the plant was brought back under control.

Connecting a control computer to another system is a modification and should only be carried out after systematic study of possible consequences (see Section 20.4.3). If made, data flow should be possible only in the outward direction (see text through the end of this section). All systems should be secure. Houses need doors. The doors on control systems are less tangible than those on houses but just as important.

If an instrument reading is faulty, operators are sometimes able to override the instrument and type in an estimated reading. Sometimes they are right, and production continues; sometimes they are wrong, and an incident occurs. Operators are usually reluctant to believe unusual readings and rush to the conclusion that the instrument is faulty, whatever the type of control (see Section 3.3.2).

Today it is usually harder than in the early days of computer control for operators to interfere with the software, override interlocks, or type in "correct" readings. However, many operators acquire keys or passwords that they should not have, in much the same way as operators have always unofficially acquired and secreted an assortment of tools and adaptors. On one plant an interlock was found to be illegally blocked: the password had been disclosed to 40 people, all of whom denied responsibility (see Section 14.5 d).

I have seen only one report of a virus in process control software and none of access by hackers. The virus was found on a Lithuanian nuclear reactor and is said to have been introduced by someone who wanted the credit for detecting and removing it. However, this does not mean virus infection or hacking will never occur, and their consequences could be much more serious than loss of accountancy data. As long as a control PES stands alone and is not connected to other systems, infection is impossible (unless a virus is present in the original software), but networking is becoming increasingly common.

Computer viruses are rather like AIDS. To avoid infection, do not promiscuously share data or disks, and keep the covers on your disks in the presence of computers whose background is unknown.

20.6 NEW APPLICATIONS

Permits-to-work could be prepared and stored on a computer. The saving in effort would not be great, but additional functions are now possible. For example:

- The computer could remind the user of any special hazards associated with this piece of equipment and its contents and the actions that should be taken.
- The computer could also remind the user of any problems encountered when the equipment was being prepared or maintained on earlier occasions.

- If a vessel is being prepared for entry, the computer could check that the number of slip-plates (blinds) to be fitted (or pipes disconnected) is the same as the number of connections shown on the drawing.
- If someone tries to take out a second permit on the same item of equipment, this would be instantly apparent, and the computer could refuse to issue it.
- Suppose a fitter has to replace a gasket during a night shift. On some plants it is easy; only one sort is used, and all the fitter has to do is select the right size. On other plants many types are used. The fitter has to get out a line diagram, find the line number, and then look up the details in a bulky equipment list. It should be possible for him to view the line diagram on a computer screen, select the line with a cursor, and have details of the line displayed, including the location of spare parts and any distinguishing marks, such as the color of the gaskets. The line diagram and equipment list will have been prepared on a computer; all that is needed is a link between the design system and the maintenance system. (Of course, we should, if possible, reduce the number of types of gaskets, nuts, bolts, etc., required even though we may use more expensive types than strictly necessary on some duties.)

Another new application under development is to give operators more information about approaching hazards. For example, if hot oil, over 100°C, is added to a storage tank containing a water layer or the oil in the tank is heated above 100°C, the water may be vaporized with explosive violence; a mixture of steam and oil will be expelled through the tank vent and may even blow the roof off the tank (see Section 12.2). If the temperature of the incoming oil or the oil in the tank approaches 100°C, then the screen could display a warning message, not merely announcing a high temperature but reminding the operator of the consequences. The reminder message could also be displayed if the operator starts up or increases the heat supply to a tank that contains a water layer. On request the system could explain why the consequences may occur and refer the operator to a plant instruction, accident report, or other document, accessible on the screen, from which the operator could find more information.

The number of possible incidents that might occur and warnings that might be given is enormous, and each plant would have to make a selection based on its own experience and that of the industry. The informa-

tion would also be accessible to designers and hazop teams, though they will probably require access to the whole accident database [17].

20.7 CONCLUSIONS

If we can learn from the incidents that have occurred on process plants controlled by computers, we may be able to prevent them from happening again. Familiar errors caused the incidents that have occurred. Accidents or process upsets wil occur in any plant, whatever the method of control, if we do not allow for foreseeable slips or equipment failures if modifications are not controlled, if operators are overloaded by too much information, if information display is poor, if controllers are set incorrectly, if warnings are ignored, or if operators are not told of changes that have been made. However, some of these errors are more likey to occur on plants controlled by computers than on conventional plants. This is because different departments may be responsible for operation of the plant and design and operation of the control system, and operating staff members may have exaggerated views of the power of the computer and a limited understanding of what it can and cannot do.

One way of improving communication between chemical and software engineers would be to combine the jobs. There is a need for engineers who are equally at home in the two fields.

REFERENCES

1. I. Nimmo, S. R. Nunns, and B. W. Eddershaw, "Lessons Learned from the Failure of a Computer System Controlling a Nylon Polymer Plant," Paper presented at Safety and Reliability Society Symposium, Altrincham, UK, Nov. 1987.
2. B. W. Eddershaw, *Loss Prevention Bulletin,* No. 088, p. 3.
3. *Chemical Safety Summary,* Vol. 56, No. 221, Chemical Industries Association, London, UK, 1985, p. 6.
4. T. A. Kletz, *Process Plants: A Handbook for Inherently Safer Design,* 2nd edition, Taylor and Francis, Washington, D.C., 1998, Chapter 7.
5. N. G. Leveson, *IEEE Software,* Vol. 7, No. 6, Nov. 1990, p. 55.
6. S. M. Englund and D. J. Grinwis, *Chemical Engineering Progress,* Vol. 88, No. 10, Oct. 1992, p. 36.
7. A. M. Wray, *New Scientist,* Vol. 119, Sept. 8, 1988, p. 61.

8. L. Bodsberg and O. Ingstad, "Technical and Human Implications of Automatic Safety Systems," Paper presented at Sixth International Symposium on Loss Prevention and Safety Promotion in the Process Industries, Oslo, Norway, 1989.
9. D. G. Mooney, "An Overview of the Shell Fluoroaromatics Explosion," *Hazards XI—New Directions in Process Safety,* Symposium Series No. 124, Institution of Chemical Engineers, Rugby, UK, 1991.
10. D. K. Lorenzo, *A Manager's Guide to Reducing Human Errors,* Chemical Manfacturers Association, Washington, D.C., 1990, p. 18.
11. P. Mahon, *Verdict on Erebus,* Collins, Auckland, New Zealand, 1984.
12. M. Shadbolt, *Reader's Digest,* Nov. 1984, p. 164.
13. R. E. Eberts, *Chemical Engineering Progress,* Vol. 82, No. 12, Dec. 1985, p. 30.
14. J. L. Lions, *Ariane 5—Flight 501 Failure,* European Space Agency, Paris, 1996.
15. N. G. Leveson, *Safeware—System Safety and Computers,* Addison-Wesley, Reading, Mass., 1996, Appendix A.
16. T. A. Kletz, et al., *Computer Control and Human Error,* Institution of Chemical Engineers, Rugby, UK, 1995, pp. 13 and 107.
17. M. Jefferson, P. W. H. Chung, and T. A. Kletz, "Learning the Lessons of Past Accidents," *Hazards XIII—Process Safety: The Future,* Symposium Series No. 141, Institution of Chemical Engineers, Rugby, UK, 1997.

ADDITIONAL READING

References 15 and 16.

Chapter 21

Inherently Safer Design

> . . . all great controversies depend on both sides sharing one false premise.
>
> —a 4th century theologian

Those who want to spend more money to make a plant safer and those who think enough has been spent share a false premise: they both assume more safety will cost more money.

Many of the incidents in this book were the result of leaks of hazardous materials, and the recommendations describe ways of preventing leaks by providing better equipment or procedures. As we have seen, equipment can fail or can be neglected, and procedures can lapse. The most effective methods, therefore, of preventing leaks of hazardous materials are to use so little that it hardly matters if it all leaks out (intensification or minimization) or to use a safer material instead (substitution). If we cannot do this and have to store or handle large amounts of hazardous material, we should store or handle it in the least hazardous form (attenuation or moderation). Plants in which this is done are said to be inherently safer because they are not dependent on added-on equipment or procedures that might fail; the hazard is avoided rather than controlled, and the safety is inherent in the design.

Because hazards are avoided, there is less need to add on protective equipment, such as interlocks, alarms, emergency isolation valves, fire insulation, water spray, etc., and the plants are therefore usually cheaper as well as safer.

The principles of inherently safer design may seem obvious, but until the explosion at Flixborough in 1974 (see Section 2.4), little thought was given to ways of reducing inventories of hazardous materials. We simply designed a plant and accepted whatever inventory was needed for that design, confident of our ability to keep it under control. Flixborough weakened our own and the public's confidence in this ability, and ten years later Bhopal almost destroyed it. The first incident described in this chapter on inherently safer design is therefore the toxic gas release at Bhopal.

My book *Plant Design for Safety—A User-Friendly Approach* [1] and References 12–15 describe many examples of ways in which plants can be made inherently safer. Note that we use the term *inherently safer,* not *inherently safe,* as we cannot avoid every hazard.

21.1 BHOPAL

The worst disaster in the history of the chemical industry occurred in Bhopal, in the state of Madhya Pradesh in central India, on December 3, 1984. A leak of methyl isocyanate (MIC) from a chemical plant, where it was used as an intermediate in the manufacture of the insecticide carbaryl, spread beyond the plant boundary and caused the death by poisoning of more than 2,000 people. The official figure was 2,153, but some unofficial estimates were much higher. In addition, about 200,000 people were injured. Most of the dead and injured were living in a shanty town that had grown up next to the plant.

The immediate cause of the disaster was the contamination of an MIC storage tank by several tons of water and chloroform. A runaway reaction occurred, and the temperature and pressure rose. The relief valve lifted, and MIC vapor was discharged to atmosphere. The protective equipment, which should have prevented or minimized the release, was out of order or not in full working order: the refrigeration system that should have cooled the storage tank was shut down, the scrubbing system that should have absorbed the vapor was not immediately available, and the flare system that should have burned any vapor that got past the scrubbing system was out of use.

The contamination of the MIC was probably the result of sabotage [2], but, as we shall see, the results would have been much less serious if less MIC had been stored, if a shanty town had not grown up close to the plant, and if the protective equipment had been kept in full working order.

21.1.1 "What You Don't Have Can't Leak"

The most important lesson to be learned from Bhopal was missed by most commentators: the material that leaked was not a product or raw material but an intermediate, and while it was convenient to store it, it was not essential to do so. Following Bhopal, the company concerned. Union Carbide, and other companies decided to greatly reduce their stocks of MIC and other hazardous intermediates. A year after the disaster, Union Carbide reported that stocks of hazardous intermediates had been reduced by 75% [3].

The product, carbaryl, was manufactured by reacting phosgene and methylamine to produce MIC, which was then reacted with alpha-naphthol. The same product can be made from the same raw materials by reacting them in a different order and avoiding the production of MIC. Phosgene is reacted with alpha-naphthol, and then the intermediate is reacted with methylamine.

21.1.2 Plant Location

If materials that are not there cannot leak, people who are not there cannot be killed. The death toll at Bhopal—and at Mexico City (see Section 8.1.4) and Sao Paulo (see Section 9.1.8)—would have been lower if a shanty town had not been allowed to grow up near the plant. It is, of course, much more difficult to prevent the spread of shanty towns than of permanent dwellings, but nevertheless we should try to do so by buying and fencing land if necessary (or removing the need to do so, as described above).

21.1.3 Keep Incompatible Materials Apart

The MIC storage tank was contaminated by substantial quantities of water and chloroform—up to a ton of water an 1½ tons of chloroform—and this led to a complex series of runaway reaction [4]. The precise route by which water entered the tank is unknown; several theories have been put forward, and sabotage seems the most likely [2], though whoever deliberately added the water may not have realized how serious the consequences would be. Hazard and operability studies (Section 18.7) are a powerful tool for identifying ways in which contamination and other

unwanted deviations can occur, and since water was known to react violently with MIC, it should not have been allowed anywhere near it.

21.1.4 Keep Protective Equipment in Working Order—and Size It Correctly

As already stated, the refrigeration, flare, and scrubbing systems were not in full working order when the leak occurred. In addition, the high temperature and pressure on the MIC tank were at first ignored because the instruments were known to be unreliable. The high-temperature alarm did not operate, as the set-point had been raised and was too high. One of the main lessons of Bhopal is, therefore, the need to keep protective equipment in working oder. Chapter 14 describes some other accidents that illustrate this theme.

It is easy to buy safety equipment. All we need is money, and if we make enough fuss we get the equipment in the end. It is much more difficult to make sure the equipment is kept in full working order when the initial enthusiasm has faded. All procedures, including testing and maintenance procedures, are subject to a form of corrosion more rapid than that which affects the steelwork and can vanish without trace once managers lose interest. A continuous auditing effort is needed to make sure that procedures are maintained.

Sometimes managers and supervisors lose interest, and unknown to them, operators stop carrying out procedures. However, shutting the flare system down for repair and taking the refrigeration system out of use were not decisions operators would make on their own. Managers must have made these decisions and thus showed a lack of understanding and/or commitment.

The refrigeration, scrubbing, and flare systems were probably not big enough to have prevented a discharge of MIC of the size that occurred, but they would have reduced the amount discharged to atmosphere. The relief valve was not big enough to handle the two-phase flow of liquid and vapor it was called upon to handle, and the tank was distorted by the rise in pressure, although it did not burst. Protective systems cannot be designed to handle every conceivable eventuality, but nevertheless Bhopal does show the need to consider a wide range of circumstances, including contamination, when highly toxic materials such as MIC are handled. It also shows the need, when sizing relief valves, to ask if two-phase flow will occur.

21.1.5 Joint Ventures

The Bhopal plant was half-owned by a U.S. company and half-owned locally. The local company was responsible for the operation of the plant as required by Indian law. In such joint ventures, it is important to be clear who is responsible for safety—in both design and operation. The technically more sophisticated partner has a special responsibility and should not go ahead unless it is sure that the operating partner has the knowledge, experience, commitment, and resources necessary for handling hazardous materials. It cannot shrug off responsibility by saying that it is not in full control.

21.1.6 Training In Loss Prevention

Bhopal—and many of the other incidents described in this book—leads us to ask if those who designed and operated the plant received sufficient training in loss prevention, as students and from their employers. In the UK, all chemical engineering undergraduates get some training in loss prevention, but this is not the case in most other countries, including the United States. Loss prevention should be included in the training of all engineers; it should not be something added onto a plant after design, like a coat of paint, but an integral part of design. Whenever possible, hazards should be removed by a change in design, such as a reduction in inventory, rather than by adding on protective equipment. While we may never use some of the skill and knowledge we acquire as students, every engineer will have to make decisions about loss prevention, such as deciding how far to go in removing a hazard [5].

At Bhopal, there had been changes in staff and reductions in manning, and the new recruits may not have been as experienced as the original team. However, I do not think that this contributed significantly to the cause of the accident. The errors that were made, such as taking protective equipment out of commission, were basic ones that cannot be blamed on inexperience of a particular plant.

21.1.7 Public Response

Bhopal showed the need for companies to collaborate with local authorities and emergency services in drawing up plans for handling emergencies.

Inevitably, Bhopal produced a great deal of public reaction throughout the world but especially in India and the United States. There have been calls for greater control (a paper titled "A Field Day for the Legislators" [6] listed 32 U.S. government proposals or activities and 35 international activities that had been started by the end of 1985) and attempts to show that the industry can put its own house in order (for example, the setting up of the Center for Chemical Process Safety by the American Institute of Chemical Engineers and of the Community Awareness and Response program by the Chemical Manufacturers Association).

Terrible though Bhopal was, we should beware of overreaction or suggestions that insecticides, or the whole chemical industry, are unnecessary. Insecticides, by increasing food production, have saved more lives than were lost at Bhopal. But Bhopal was not an inevitable result of insecticide manufacture. By better design and operations and by learning from experience, further Bhopals can be prevented. Accidents are not due to lack of knowledge but failure to use the knowledge we have. Perhaps this book will help spread some of that knowledge.

21.2 OTHER EXAMPLES OF INHERENTLY SAFER DESIGN

21.2.1 Intensification

The most effective way of designing inherently safer plants is by intensification, that is, using or storing smaller amounts of hazardous material so that the effects of a leak are less serious. When choosing designs for heat exchangers, distillation columns, reactors, and all other equipment, we should, whenever possible, choose designs with a small inventory or hold-up of hazardous material. References 1 and 12–15 describe some of the changes that are possible. Intensification is easy to apply on a new plant, but its application to existing plants is limited unless we are prepared to replace existing equipment. However, as we have seen, stocks of hazardous intermediates can be reduced on existing plants. When the product of one plant is the raw material of another, stocks can be reduced by locating both plants on the same site, and this also reduces the amount of material in transit.

One company found that it could manage without 75% of its product storage tanks, though in this case the tanks, not the product, were hazardous (see Section 9.2.1 g).

Nitroglycerin (NG) production provides a good example of the reductions in inventory that can be achieved by redesign. It is made from glycerin and a mixture of concentrated nitric and sulfuric acids. The reaction is very exothermic; if the heat is not removed by cooling and stirring, an uncontrollable reaction is followed by explosive decomposition of the NG.

The reaction was originally carried out batchwise in large stirred pots each containing about a ton of material. The operators had to watch the temperature closely. and to make sure they did not fall asleep, they sat on one-legged stools. next to the reactors.

If we were asked to make this process safer, most of us would add onto the reactor instruments for measuring temperature, pressure, flows, rate of temperature rise. and so on and then use these measurements to operate valves that stopped flows, increased cooling, opened vents and drains, and so on. By the time we had finished, the reactor would hardly be visible beneath the added-on protective equipment. However, when the NG engineers were asked to improve the process, they asked why the reactor had to contain so much material. The obvious answer was because the reaction is slow. But the chemical reaction is not slow. Once the molecules come together they react quickly. It is the chemical engineering—the mixing—that is slow. They therefore designed a small well-mixed reactor, holding only about a kilogram of material, which achieves about the same output as the batch reactor. The new reactor resembles a laboratory water pump. The rapid flow of acid through it creates a partial vacuum, which sucks in the glycerin through a side-arm. Very rapid mixing occurs. and by the time the mixture leaves the reactor. reaction is complete. The residence time in the reactor was reduced from 120 minutes to 2 minutes. and the operator could then be protected by a blast wall of reasonable size. Similar changes were made to the later stages of the plant where the NG is washed and separated. The reactor, cooler, and centrifugal separator together contain 5 kg of NG [16].

Whatever the method of production, the product, NG. is still hazardous, and it is now being replaced by safer explosives. Increasingly, quarries now use explosives prepared at the point of use by mixing two nonexplosive ingredients.

Intensification, when practicable, is the preferred route to inherently safer design, as the reduction in inventory results in a smaller and thus cheaper plant. This is, in addition to the reduction in cost. achieved by reducing the need for added-on protective equipment.

21.2.2 Substitution

If intensification is not possible, we should consider substitution, that is, replacing a hazardous material by a less hazardous one. For example, benzene, once widely used as a solvent, is immediately toxic in high concentrations and produces long-term toxic effects in low concentrations. Other solvents, such as cyclohexane, can often be used instead. Better still, nonflammable or high-flash-point solvents may be suitable. In the food industry, supercritical carbon dioxide is now widely used instead of hexane for decaffeinating coffee and extracting hops. It can also be used for degreasing equipment [7]. Similarly, nonflammable or high-flash-point heat transfer fluids should be used whenever possible instead of those that have low flash points.

Supplier of helium operate a recovery service. Helium contaminated with air and/or nitrogen is returned to them and is purified by passing the gas through a carbon bed cooled to −196°C by a jacket of boiling liquid nitrogen. The oxygen and nitrogen are absorbed by the carbon. The returned helium usually contains far more nitrogen than oxygen. However, one batch of returned helium contained 1.3% nitrogen and 2.2% oxygen. As the oxygen has a higher boiling point (−183°C), it condensed out preferentially, and the gas absorbed on the top of the carbon bed was 85% oxygen. The carbon-oxygen mixture exploded, causing extensive blast and missile damage but, fortunately, no injuries. Minor mechanical shock could have detonated the mixture.

None of the people on the plant realized that a change in feed composition could be hazardous. However, when they told other helium suppliers what had happened, two earlier unpublished incidents came to light. This third incident might not have occurred if the people who failed to publicize the earlier incidents had been more open.

Analysis procedures are now more rigorous. In addition, an example of substitution, silica gel, which does not react with oxygen, is used as the absorbent instead of carbon. Silica gel is less efficient but inherently safer [8].

As in the case of Bhopal (Section 21.1.1), a different chemical route can sometimes be substituted for one that has hazardous consequences. Here is an example from another industry. Pastry dough is made, at home and industrially, by mixing flour and fat and then adding water. If used to cover a pie, it is liable to crack or slump. According to International Patent Application No. 96/39852, these disasters can be prevented by

emulsifying the water and fat, with the help of an emulsion stabilizer, and then adding the flour [17].

21.2.3 Attenuation

A third method of making plants inherently safer is attenuation—using hazardous materials in the least hazardous form. For example, while small quantities of liquefied toxic or flammable gases such as chlorine, ammonia, and propane are usually stored under pressure at atmospheric temperature, large quantities are usually stored at low temperature at or near atmospheric pressure. Because the pressure is low, the leak rate through a hole of a given size is smaller, and because the temperature is low, evaporation is much less (see Section 8.1.5). The possibility of a leak from the refrigeration equipment has to be considered as well as the possibility of a leak from the storage vessel, and for this reason only large quantities are refrigerated.

Another example of attenuation is storing or transporting a hazardous material in a solvent. Thus, acetylene has been stored and transported for many years as a solution in acetone, and many organic peroxides, which are liable to decompose spontaneously, are stored and transported in solution.

21.2.4 Limitation of Effects

A fourth road to inherently safer design is limitation of effects, by equipment design or by limiting the energy available, rather than by adding on protective equipment. For example, many spillages of liquefied petroleum gas are due to overfilling of storage vessels and discharge of liquid from a relief valve that is not connected to a flare system. If the filling pumps can be rated so that their closed-head delivery pressure is below the set-point of the relief valves (or the vessels designed so that they can withstand the delivery pressure), then the relief valves will not lift when the vessels are filled.

Similarly, overheating can be prevented by using a heating medium at a temperature too low to be hazardous. For example, corrosive liquids are often handled in plastic (or plastic-coated) tanks heated by electric immersion heaters. If the liquid level falls, exposing part of the heater, the tank wall may get so hot that it catches fire. One insurance company

reported 36 such fires in two years, many of which spread to other parts of the plants. Five were due to failure of a low-level interlock.

The inherently safer solution is to use a source of heat that is not hot enough to ignite the plastic, for example, hot water, low-pressure steam, or low-energy electric heaters [9].

If unstable chemicals have to be kept hot, the heating medium should be incapable of overheating them. Some acidic dinitrotoluene should have been kept at 150°C, as it decomposes at higher temperatures. It was heated by steam at 210°C for ten days in a closed pipeline and decomposed explosively [10].

21.2.5 Seveso

The use of an unnecessarily hot heating medium led to the runaway reaction at Seveso, Italy, in 1976, which caused a fallout of dioxin over the surrounding countryside, making it unfit for habitation. Although no one was killed, it became one of the best-known chemical accidents, exceeded only by Bhopal, and had far-reaching effects on the laws of many countries.

A reactor containing an uncompleted batch of 2,4,5-trichlorophenol (TCP) was left for the weekend. Its temperature was 158°C, well below the temperature at which a runaway reaction can start (believed at the time to be 230°C but possibly as low as 185°C). The reaction was carried out under vacuum, and the reactor was heated by an external steam coil supplied with exhaust steam from a turbine at 190°C and a gauge pressure of 12 bar (Figure 21.1). The turbine was on reduced load, as various other plants were also shutting down for the weekend (as required by Italian law), and the temperature of the steam rose to about 300°C. The temperature of the bulk liquid could not get much above 158°C because of its heat capacity, and so below the liquid level there was a temperature gradient through the walls of the reactor, 300°C on the outside, 158°C on the inside. Above the liquid level, the walls were at 300°C right through.

When the steam was isolated and, 15 minutes later, the stirrer was switched off, heat passed by conduction and radiation from the hot wall above the liquid to the top 10 cm or so of the liquid, which became hot enough for a runaway to start. If the steam had been cooler, 185°C or less, the runaway could not have occurred [11] (see also Section 10.4.6).

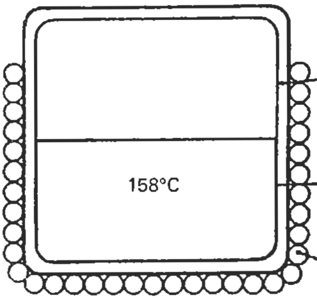


Figure 21-1. The Seveso reactor.

21.2.6 Existing Plants

As already stated, it is difficult to introduce inherently safer designs on existing plants, though storage can often be reduced. However, one company improved the inherent safety of an acquired pant, which contained a unit for the manufacture of phosgene. Improvements to the reliability of the control equipment made it possible to reduce in-plant storage; buying purer carbon monoxide, one of the raw materials, made it possible to eliminate parts of the purification section (thus simplifying as well as intensifying); and changing the chlorine supply from liquid to gas reduced the chlorine inventory by 90% [18].

21.3 USER-FRIENDLY DESIGN

A related concept to inherently safer design is user-friendly design: designing equipment so that human error or equipment failure does not have serious effects on safety (and also on output or efficiency). While we try to prevent human errors and equipment failures, only very low failure rates are acceptable when we are handling hazardous materials, and, as this book has shown, it is hard to achieve them. We should, therefore, try to design so that the effects of errors are not serious. The following are some of the ways in which we can accomplish this:

- By simplifying designs: complex plants contain more equipment that can fail, and there are more ways in which human errors can occur.
- By avoiding knock-on effects: for example, if storage tanks have weak seam roofs, an explosion or overpressuring may blow the roof off, but the contents will not be spilled (see Section 5.2).

- By making incorrect assembly impossible (for an example, see Section 9.1.3).
- By making the status of equipment clear. Thus, figure-8 plates are better than slip-plates, as the position of the former is obvious at a glance, and valves with rising spindles are better than valves in which the spindle does not rise. Ball valves are friendly if the handles cannot be replaced in the wrong position.
- Using equipment that can tolerate a degree of misuse. Thus, fixed pipework is safer than hoses (see Section 7.1.6), and fixed pipework with expansion loops is safer than expansion joints (bellows).

Reference 1 gives more examples.

REFERENCES

1. T. A. Kletz, *Process Plants: A Handbook for Inherently Safer Design,* 2nd edition, Taylor and Francis, Washington, D.C., 1998.
2. A. Kalelkar, "Investigation of Large Magnitude Incidents: Bhopal as a Case Study," *Preventing Major Chemical and Related Process Accidents,* Symposium Series No. 110, Institution of Chemical Engineers, Rugby, UK, 1988.
3. *Chemical Insight,* late Nov. 1985, p. 1.
4. *Bhopal Methyl Isocyanate Incident: Investigation Team Report,* Union Carbide Corporation, Danbury, Conn., Mar. 1985.
5. T. A. Kletz, *Plant/Operations Progress,* Vol. 7, No. 2, Apr. 1988, p. 95.
6. W. Stover, "A Field Day for the Legislators," *The Chemical Industry after Bhopal,* Proceedings of a symposium, IBC Technical Services, London, Nov. 7–8, 1985.
7. *Swedish Work Environment Fund Newsletter,* No. 2, 1992.
8. J. W. Hempseed and R. W. Ormsby, *Plant/Operations Progress,* Vol. 10, No. 3, July 1991, p. 184.
9. *Sentinel,* International Risk Insurers, 3rd quarter 1981.
10. *Loss Prevention Bulletin,* No. 088, p. 13.

11. T. A. Kletz, *Learning from Accidents,* 2nd edition, Butterworth-Heinemann, Oxford, UK, 1994, Chapter 9.

12. D. A. Crowl (editor), *Inherently Safer Chemical Processes—A Life Cycle Approach,* AIChE, New York, 1996.

13. *International Conference and Workshop on Process Safety Management and Inherently Safer Processes,* AIChE, New York, 1996.

14. *Guidelines for Engineering Design for Process Safety,* AIChE, New York, 1993, Chapter 2.

15. S. M. Englund, "Process and Design Opportunities for Inherently Safer Plants," in V. M. Fthenakis (editor), *Prevention and Control of Accidental Releases of Hazardous Gases,* Van Nostrand Reinhold, New York, 1993.

16. N. A. R. Bell, "Loss Prevention in the Manufacture of Nitroglycerin," *Loss Prevention in the Process Industries,* Symposium Series No. 34, Institution of Chemical Engineers, Rugby, UK, 1971.

17. *Chemistry and Industry,* No. 14, July 21, 1997, p. 548.

18. R. Gowland, *1996 Process Safety Progress,* Vol. 15, No. 1, Spring 1996, p. 52.

ADDITIONAL READING ON BHOPAL

P. Shrivastava, *Bhopal—Anatomy of a Crisis,* Ballinger, Cambridge, Mass., 1987.

S. Varadarajah, *Report on Scientific Studies on the Factors Related to Bhopal Toxic Gas Leakage,* Indian Planning Commission, New Delhi, India, Dec. 1985.

S. Hazarika, *Bhopal—The Lessons of a Tragedy,* Penguin Books, London, 1987.

T. A. Kletz, *Learning from Accidents,* 2nd edition, Butterworth-Heinemann, Oxford, UK, 1994, Chapter 10.

Chapter 22

Reactions—Planned and Unplanned

Famous last words: "I didn't see an exotherm in the lab"; "I only saw a little bit of foaming"; "It goes a bit brown if you leave it in the oven for too long."

—Chilworth Technology

Many accidents, particularly on batch plants, have been due to runaway reactions, that is, reactions that get out of control. The reaction becomes so rapid that the cooling system cannot prevent a rapid rise in temperature, and/or the relief valve or rupture disc cannot prevent a rapid rise in pressure, and the reactor ruptures. Examples are described in the chapter on human error (Sections 3.2.1 e and 3.2.8), although the incidents were really due to poor design, which left traps into which someone ultimately fell.

The number of reactions that can run away is enormous, *Bretherick's Handbook of Reactive Chemical Hazards* [1] lists about 4,700 chemicals that have been involved in hazardous reactions of one sort or another, and there are more than 20,000 cross-references to entries involving more than one chemical. It is an essential work of reference for the chemist, the process engineer, and everyone involved in process safety. All I can do here is give a few examples to illustrate the reasons why runaways occur.

22.1 LACK OF KNOWLEDGE

This is, or was at one time, the major cause of runaway reactions. After many years of safe operation, a chemical or a reaction mixture gets a little hotter than usual or is kept warm for a little longer than usual, and a runaway occurs. Today there is little excuse for such runaways, as many methods are available for testing both pure substances and reaction mixtures. They include accelerating rate calorimetry (ARC), differential scanning calorimetry, and reaction calorimetry. There are also methods for determining the size of relief valve, rupture disc, or vent required. Expert advice is needed on the most suitable technique for each case. If process conditions are changed, then further testing may be necessary. Section 2.6 (d) describes a slight change in operating conditions, which led to a violent explosion.

Safe operation for many years does not prove that a reaction will not run away. Unknown to the operators, the plant may be close to the conditions under which it becomes unstable, and a slight change in pressure, temperature, or concentration, too small to cause concern, may take it over the brink. The operators are blind men walking along the edge of a precipice, as the following incidents illustrate.

(a) Some zoalene (3,5-dinitro-ortho-toluamide), a poultry food additive, was left standing for longer than usual after drying. After 27 hours a devastating explosion occurred. Tests by accelerating rate calorimetry (ARC) showed that zoalene could self-heat to destruction if held at 120°–125°C for 24 hours.

The company had started to test by ARC, then a new technique, all the chemicals it handled. At the time of the explosion the company had tested 5% of them. It had no reason to give zoalene priority, as other tests and 17 years of manufacturing experience had given no inkling of its instability. The official report on the explosion concluded, "There appears to be no substantial grounds for criticizing the management or operating personnel for undertaking and conducting the operation that led to the explosion in the way they did" [2]. The conclusion would, of course, have been different if the zoalene had blown up several years later, after the company had time to test all its chemicals.

(b) As the result of a steam leak into a reactor jacket, some nitrobenzene sulfonic acid was held for 11 hours at 150°C. Decomposition

occurs above 145°C, and a violent explosion expelled the reactor from the building. At a time, decomposition was believed to occur only above 200°C [3].

(c) A solution of ferric chloride in a solvent was manufactured by suspending iron powder and adding chlorine. The process was tested by ARC and on a pilot scale and then transferred to a full-scale reactor (1.2 m diameter by 2 m tall). During the third batch, a devastating explosion occurred, killing 2 people and injuring 50.

The control of the reaction was based on the assumption that stopping the flow of chlorine would stop all reaction; this was true on the pilot unit but not on the full-scale plant. On the pilot unit, there was no stirrer, as the incoming chlorine gave sufficient mixing. When chlorine addition stopped, mixing also stopped and so did the reaction. On the full-scale plant, a stirrer was necessary, and this continued in operation after chlorine addition stopped. In addition, on the pilot unit the cooling was sufficient to hide any continuing reaction that did occur.

Stirring was attempted during the ARC tests, but the iron powder interfered with the mechanically coupled stirrer [4].

(d) Many incidents have occurred because designers failed to realize that as the volume of a reactor is increased, the surface area and thus the heat loss do not increase in proportion. If the height of a reactor is doubled and the shape stays the same, then the volume increases eight times, but the surface area increases only four times.

A reaction was believed to be thermally neutral, as no rise in temperature was observed in the laboratory. No cooling was provided on the pilot plant, and the first batch developed a runaway. Fortunately the relief valve was able to handle it. Subsequent research showed that the reaction developed 2 watts/kg/°C. Laboratory glassware has a heat loss of 3–6 watts/kg/°C, so no rise in temperature occurred. On the 2.5-m^3 pilot plant reactor, the heat loss was only 0.5 watt/kg/°C [21]. Reference 22 lists heat losses and cooling rates for vessels of various sizes.

(e) An unusual cause of a runaway reaction: thieves tried to burn their way through the steel door of a fireworks store with an oxyacetylene torch. The building, made of concrete 12 in. thick, was reduced to rubble [23].

22.2 POOR MIXING

(a) Section 3.2.8 described a runaway that occurred because a valve in a reactor circulation line was closed. As a result there was no mixing, and the incoming reactant formed a separate layer. When someone opened the valve, the two layers were suddenly mixed, with a catalyst, and reacted violently. Even though two liquids are miscible, they may still layer.

Many similar incidents have occurred when a stirrer or circulating pump stopped. For example, an acidic waste stream in a tank was neutralized with chalk slurry. The operator realized that the liquid going to drain was too acidic. Looking around, he then found that the stirrer had stopped. He switched it on again. The acid and chalk, which had formed two separate layers, reacted violently, and the gas produced blew the bolted lid off the tank.

(b) An aromatic hydrocarbon was being nitrated by slowly adding a mixture of nitric and sulfuric acids. After several hours the operator discovered the temperature had not risen. He noticed the stirrer had stopped and switched it on. Almost at once he realized that this could start a runaway reaction; he switched off the stirrer, but it was too late. Within 20 seconds fumes were coming out of the vent on the reactor. He went down to the floor below to open the drain valve, but the fumes were so thick he could not see what he was doing. Wisely, he decided to leave the area. Five minutes later the vessel burst. The lid ended up 15 m away, and the rest of the reactor was propelled several meters onto the ground [5].

Failure of a reactor stirrer or circulation pump should automatically isolate the supply of incoming liquid. If all the reactants have already been added and mixing failure is still hazardous, then the action to be taken should be agreed in advance, for example, increasing cooling, adding a quenching agent, or dumping the contents.

(c) If there is no mixing in a reactor, the temperature measurements will indicate the temperature at the point of measurement, but it may be different in other parts of the bulk liquid. A reactor was provided with a quench water system; if the contents got too hot, water could be added from a hose. A power failure caused the stirrer to stop. The operator watched the temperature. As it was falling

he did nothing. After a while it started to rise; before he could connect up the water supply, the rupture disc failed, and soon afterward the reactor blew up.

No accident has a simple cause. In this case a contributory factor was the inexperience of the operator, who had to ask someone to show him how the quench system worked. It had not been used for several years. Emergency equipment is usually used infrequently, and without regular training, people forget (or never learn) how to use it [6].

(d) A devastating explosion, which killed 46 people including 19 members of the public, destroyed a trinitrotoluene (TNT) factory in Ashton, near Manchester, UK, during the first World War. During the final stage of production, the addition of nitric acid to convert dinitrotoluene to TNT, the nitrator pan (5 ft [1.5 m] tall and 5 ft diameter) started to give off nitric acid fumes. Acid flow was stopped and so was the stirrer, but nevertheless the contents boiled over. Hot acid fell onto the wooden staging around the pan, starting a fire. Soon afterward the stocks of TNT in surrounding equipment and in drums exploded.

At the time of the explosion, the wooden stagings were being replaced by iron ones, but the work was going slowly, as the materials needed were rationed and the Munitions Works Board had classified the change as desirable but not absolutely necessary.

Why did the pan boil over? To improve efficiency the man in charge had reduced the amount of sulfuric acid added, along with nitric acid, during the final stage of the process. As less acid was added, the pan was not as full as usual, and for a time the top stirring blades were above the surface of the liquid. In addition, the use of less sulfuric acid made the reaction less stable. When the level rose and covered the blades, the unreacted acid started to react, the temperature rose, and a runaway reaction occurred [24, 25]. We thus see once again the unforeseen result of a process change that was not properly thought through (see Chapter 2).

(e) A similar incident occurred more recently during the sulfonation of a nitroaromatic compound. Some product from a previous batch was put into the reactor and heated to 85°C; the melted nitroaromatic and oleum were then added simultaneously and the temperature allowed to rise to 110°C.

The reactor was also used for other processes. The cooler was not adequate for one of them, so an additional coil was fitted. To make room for it, the stirrer was removed and replaced by a turbine agitator, located higher up the vessel. At a later date, when the process that needed the extra cooling was no longer used, the extra coil, which had corroded, was removed. This lowered the level in the reactor.

Six months later, during a routine maintenance check, the position of the agitator was inadvertently set at the highest position possible. At the start of the reaction, the agitator was now uncovered. The two reactants formed separate layers; the temperature fell, and the control system increased the steam supply to the reactor jacket. After a while, the rising liquid level covered the agitator, the accumulated quantities of the two hot reactants were mixed, and reaction began. The cooling system could not control the unusually high rate of reaction, the temperature rose, decomposition set in, the pressure rose, the reactor cover ruptured, and the contents overflowed like a stream of lava [26].

This incident and the previous one show how easy it is to reduce mixing inadvertently and how serious the results can be.

22.3 CONTAMINATION

The most famous case of a runaway reaction caused by contamination is Bhopal (see Section 21.1). In this case the reaction occurred in a storage vessel. It did not burst but was distorted, and the discharge of vapor was larger than the scrubbing and flare systems could have handled, even if they had been in operation.

Here are some other examples of unwanted reactions caused by contaminants [7]:

- Storage tanks containing ethylene oxide are usually inerted with nitrogen. One plant used nitrogen made by cracking ammonia. The nitrogen contained traces of ammonia, which catalyzed an explosive decomposition of the ethylene oxide. Similar decompositions have been set off by traces of other bases, chlorides, and rust.
- A storage tank containing acrolein was kept cool by circulating the liquid through a water-cooled heat exchanger. Demineralized water was normally used, but the supply failed, and water from an under-

ground borehole was used instead; it contained numerous minerals. There was a very slight leak in the heat exchanger, some water contaminated the acrolein, and the minerals catalyzed rapid polymerization. The tank exploded.

- A high-pressure air compressor drew its air from an area where oxy-acetylene welding was taking place. Small amounts of copper acetylide formed on a bronze valve and exploded.
- Unstable impurities may concentrate on certain trays in a distillation column.
- Traces of oxygen in nitrogen used for inerting can react with some products, such as butadiene and acrolein, and cause explosive polymerization. In one case, unknown to the acrolein plant, a trace of oxygen was deliberately added to the nitrogen supply at the request of another plant.
- Inhibitors are usually added to butadiene and acrolein to prevent polymerization, but the system is not foolproof. Several runaways have occurred in tank trucks or tank cars containing acrolein. As it cooled, some of the liquid crystallized, leaving the inhibitor in solution. In other cases impurities have been left behind in the bulk liquid, and their concentration has risen sufficiently to start a runaway.

Vessels are sometimes contaminated by material left over from a previous use. For example, tank trucks were filled with a waste sludge containing particles of aluminum. One day the tank truck contained some caustic soda left over from the previous load. The caustic soda reacted with the aluminum, producing hydrogen. The increase in pressure blew open an inspection port and knocked an operator onto the ground.

Another example: a solvent was put into a small reactor to remove some polymer, which was stuck to the walls. Some monomer, which was trapped behind the polymer, reacted with the solvent, and the pressure rose. Bits of polymer plugged the relief valve, and the pressure broke a glass connecting line [8].

Reactions have often taken place in waste containers because assorted substances were added indiscriminately [8]. Leaking heat exchangers can also cause contamination as described above.

A top-quality London hotel was horrified to find that its house champagne, for which it charged $60 per bottle, lost its bubbles a few moments after it was poured. At first the hotel blamed the suppliers, but

the trouble was found to be due to a trace of the detergent used to wash the glasses [27].

22.4 REACTIONS WITH AUXILIARY MATERIALS

As well as testing the reactants, as described in Section 22.1, we should also test auxiliary materials. For example, nitrogen trifluoride reacted with silica, which was used as a drying agent. Whenever a new batch of silica was installed, there was a rise in temperature, which the operators never reported and in time accepted as normal. They were walking along the precipice described in Section 22.1, and one day the temperature rise got out of control.

22.5 POOR TRAINING OR PROCEDURES

An operator was told to add a reactant over a certain period of time. He started to add it too slowly. Finding that he was getting behind, he added the rest too quickly, and a runaway occurred. Fortunately, in this case, the relief device controlled the situation, and the reactor did not rupture, though product was wasted. It may be necessary to specify the rate of addition as well as the time of addition.

Operators were told to add a reactant at 45°C over a period of 1–1½ hours. They believed this to be impossible, as the heater was not powerful enough, so they decided to add it at a lower temperature and heat the material in the reactor. They did not tell anyone. This went on for a long period of time and, unknown to the supervisor, became the accepted practice. Again they were on the edge of a precipice, and ultimately a runaway reaction occurred with emission of toxic fumes.

Unfortunately, if people are given instructions that are impossible or that they think are impossible to carry out, they do not like to tell their supervisors, and so they often just do the best they can. However, in this case if proper records had been kept and the supervisor examined them, he would have noticed that the addition temperature was wrong.

Runaways have also occurred when operators added the wrong material to a reactor, often because different materials had similar names, were stored in similar drums, or were poorly labeled (see Chapter 4).

A batch distillation column, used for distilling nitrotoluene, had not been cleaned for 30 years. A buildup of sludge caused some problems, or

so it was believed, and those in charge decided to clean the column with live steam. The operators were told not to let the sludge get above 90°C, but there was no way they could measure its temperature; all they could measure was the temperature of the vapor in the still. The sludge got much hotter, and a runaway reaction occurred. A ball of flame came out of an open manhole on the base of the still, engulfed the control room—a wooden building (!)—25 m away, crossed a parking lot, and reached the office block. Five men were killed; four of them were in the control room. The company had to pay fines and costs of $600,000 [9].

Nitration has been described as the "most widespread and powerfully destructive industrial unit process operation" [10].

22.6 USE-BY DATES

We are used to seeing sell-by or use-by dates on food. Some chemicals also have, or ought to have, use-by dates on them. The best known are ethers; on standing, they form peroxides, which can explode if subjected to shock. Ethers should not be kept for more than limited periods—six months in the case of dimethyl and other low-molecular-weight ethers. This has been known for many years, and Bretherick [11] gives references to a number of explosions that occurred because ethers were kept for too long. A particularly tragic accident befell a research chemist. He tried to open a bottle of isopropyl ether by holding it against his stomach and twisting the cap. The bottle exploded, injuring him so severely that he died two hours later [12]. Nevertheless, according to a recent report from the U.S. Department of Energy [13], 21 containers of dimethyl ether more than 21 months old were found in one of its laboratories.

The U.S. Department of Energy also points out that polyethylene bottles containing corrosive chemicals may deteriorate with prolonged use [14].

Other limited-life chemicals listed by Bretherick are bleaching powder ("Material which has been stored for a long time is liable to explode on exposure to sunlight or on overheating of tightly packed material in closed containers" [15]) and aqua regia, a 1:4 mixture of nitric and sulfuric acids used for cleaning ("Aqua regia decomposes with evolution of gas and should not be stored in tightly closed bottles [and preferably not at all]" [16]).

A dilute solution of hydroxylamine nitrate and nitric acid was left in a vented tank for four years. Evaporation caused the concentration of the

chemicals to rise until they started to react together. They produced so much steam and gas that they blew the lid off the tank. In another incident, the same mixture, plus hydrazine, was trapped between two valves. Decomposition ruptured a gasket. Chemicals should be removed from vessels that are no longer in use [28, 29].

Oil spillages onto warm, absorbent materials, such as insulation, also have a limited life (see Sections 7.3.2 and 12.4.4). The oil soon decomposes to materials with a low auto-ignition temperature and self-ignites. As many insulation fires have started in this way, oil-soaked insulation should be removed without delay. Linseed oil ignites particularly easily. This has been known since at least 1925; nevertheless, in 1965 some cloths used to apply linseed oil to laboratory benches were not burned as directed but dropped into a waste bin. A fire started after a few hours and destroyed the laboratory [17]. Reference 18 lists substances that are liable to self-heat, and Reference 19 includes references to a number of incidents that have occurred involving substances as diverse as wood shavings, tobacco, milk powder, and soap powder.

A manufacturer of ethylene oxide received some old returned cylinders in which the ethylene oxide had partly polymerized, sealing the valves. They were taken to an explosives testing site and blown up [20].

REFERENCES

1. P. G. Urben (editor), *Bretherick's Handbook of Reactive Chemical Hazards,* 5th edition, Butterworth-Heinemann, Oxford, UK, 1995.
2. Health and Safety Executive, *The Explosion at the Dow Chemical Factory, King's Lynn, 27 June 1976,* Her Majesty's Stationery Office, London, Mar. 1977.
3. *Case Histories of Accidents in the Chemical Industry,* Vol. 3, Manufacturing Chemists Association, Washington, D.C., 1970, p. 111.
4. E. S. De Haven and T. J. Dietsche, *Plant/Operations Progress,* Vol. 9, No. 2, Apr. 1990, p. 131.
5. T. Kotoyori, *Journal of Loss Prevention in the Process Industry,* Vol. 4, No. 2, p. 120.
6. *Loss Prevention Bulletin,* No. 098, Apr. 1991, p. 7.

7. R. Grollier Baron, "Hazards Caused by Trace Substances," *Seventh International Symposium on Loss Prevention and Safety Promotion in the Process Industries,* Taormina, Italy, May 4–8, 1992.
8. M. A. Capraro and J. H. Strickland, *Plant/Operations Progress,* Vol. 8, No. 4, Oct. 1989, p. 189.
9. Health and Safety Executive, *The Fire at Hickson and Welch Ltd.,* HSE Books, Sudbury, UK, 1994.
10. Reference 1, Vol. 2, p. 231.
11. Reference 1, Vol. 2, p. 120.
12. *Case Histories of Accidents in the Chemical Industry,* Vol. 2, Manufacturing Chemists Association, Washington, D.C., 1966, p. 6.
13. *Safe Chemical Storage,* Bulletin 91-2, DOE/EH-0168, U.S. Dept. of Energy, Washington, D.C., Feb. 1991.
14. *Polyethylene Bottles Containing Corrosive Chemicals May Deteriorate with Prolonged Use,* Bulletin 89-1, DOE/EH-0094, U.S. Dept. of Energy, Washington, D.C.. Aug. 1989.
15. Reference 1, Vol. 2, p. 56.
16. Reference 1, Vol. 2, p. 43.
17. Reference 1, Vol. 2, p. 185.
18. J. Bond, *Sources of Ignition,* Butterworth-Heinemann, Oxford, UK, 1990, Appendix 2.6.
19. Reference 1, Vol. 2, p. 341.
20. E. S. Hunt, *Loss Prevention,* Vol. 6, 1972, p. 140.
21. *Process Safety News,* No. 3, Chilworth Technology, Southampton, UK, Autumn 1996/Winter 1997, p. 1.
22. J. Singh, *Chemical Engineering,* May 1997, p. 92.
23. *The Times* (London), 1996 (precise date unknown).
24. J. Billings and D. Copland, *The Ashton Munitions Explosion,* Tameside Leisure Services, Stalybridge, UK.
25. *Explosion of TNT at Ashton-under-Lyne,* Ref. No. MUN7/37 XC/B/8909, Public Records Office, London.

26. *Thermal Process Safety,* Expert Commission for Safety in the Swiss Chemical Industry, Basle, Switzerland, 1993.
27. *Daily Telegraph Business News* (London), Nov. 5, 1994.
28. *Operating Experience Weekly Summary,* No. 97-21, Office of Nuclear and Safety Facility, U.S. Dept. of Energy, Washington, D.C., 1997, p. 1.
29. *Chemical Explosion at Hanford,* Safety Alert No. 97-1, U.S. Dept. of Energy, Washington, D.C., 1997.

ADDITIONAL READING ON RUNAWAY REACTIONS

J. Barton and R. Rogers, *Chemical Reaction Hazard,* 2nd edition, Institution of Chemical Engineers, Rugby, UK, 1997.

Appendix 1

Relative Frequencies of Incidents

The following is a summary of a recent paper [1] that discusses the relative frequencies of many of the incidents described in this book. It is based on an analysis of almost 500 incidents in the oil and chemical industries. I have added references to the book when accounts of similar incidents are collected in one place, but when they are scattered, for example, those referring to drains and vents, please consult the index.

- Half the incidents were maintenance-related in some way: 15% were associated with shutdowns, 14% with startups, 10% with maintenance, and 11% with actions taken to avoid shutdowns due to faulty equipment.
- Well-conducted hazard and operability studies (Chapter 18) could have prevented about half the incidents (but only 40% in the 1980s and 1990s). The incidents they could not have prevented include, for example, mechanical failures and installation of the wrong material of construction.
- Of the incidents, 22% occurred in storage and blending areas. Of these incidents:
  - 10% were due to the presence of flammable mixtures in the vapor space (see Section 5.5.4).
  - Another 10% were due to mixing a hot liquid and a cold volatile one, usually hot oil and water (foamovers) (see Sections 12.2 and 17.12).

- Nearly 10% were due to leakage through seals on floating roof tanks as the vapor pressure was too high (see Section 5.5).
- Other frequent causes were poor design or use of drains and vents (see index) and freezing of water (see Section 9.1.1).

- After storage tanks, the equipment most often involved was pressure vessels, 16%, and piping, 12% (of which a third was due to corrosion). (Chapter 9 attributes many more failures to piping.)
- Liquefied petroleum gas (LPG) was involved in 17% of the incidents (see Chapter 8), followed by heavy oils (see Section 12.4), gasoline, hydrogen, and hydrocarbon gases. Heavy oils are involved in so many incidents because they are often handled above their auto-ignition temperature and because they are involved in foamovers.
- Ignition: in 23% of the cases where this occurred, the source was unknown; in about a third of the incidents in which the source was known, it was auto-ignition. Other common sources were flames, hot surfaces, sparks, lightning, static electricity and electrical equipment. In many cases conditions changed after a permit-to-work had been issued (see Section 1.3.2).
- "Primary causes": 10% of the incidents were due to runaway reactions (Chapter 22), caused mainly by loss of utilities, reverse flow (Chapter 18), charging the wrong reactant, plugging of catalyst beds, unexpected freezing that removed an inhibitor (compare item 5.3 l) and overheating. Of the incidents, 8% were due to corrosion and erosion (Chapter 16), another 8% to modifications (Chapter 2), 7% to the use of the wrong material of construction (Section 16.1), 5% to the failure of safety instruments (Chapter 14) and relief valves (Section 10.4), 5% to vibration, 5% to leaks from drains and vents, 5% to faults in relief and flare systems, 5% to overheating (of which half were furnace tube ruptures), and 3.5% to each of the following: poor isolation for maintenance (Section 1.1), poor identification for maintenance (Section 1.2), freezing (Section 9.1.1), failure of check valves, and finally, process fluids having a higher vapor pressure than assumed during design.
- "Responsibility": 60% of the incidents could have been prevented by better process design. A third of the incidents could have prevented by better operating procedures (including handwritten temporary ones) or by replacing missing ones. Of the incidents, 20% were attributed to operator error, including errors due to poor training but

also errors due to poor labeling or layout, which can be prevented by better design (see Chapters 3 and 4). Of the incidents, 16% could have been prevented by better inspection and 10% by better mechanical design.

REFERENCE

1. I. M. Duguid, *Loss Prevention Bulletin,* No. 142, Aug. 1998, p. 3; No. 143, Oct. 1998, p. 3; and No. 144, Dec. 1998, p. 26.

Appendix 2

Final Thoughts

WHY SHOULD WE PUBLISH ACCIDENT REPORTS?

Some of the reports in this book have come from my own experience. Others were supplied by other people, either privately or through publications. I hope they will help you prevent similar incidents on your plant.

Almost every reader will, if not now then in the future, experience incidents from which others can learn. In return for what you have learned from this book, I hope you will publish accounts of your incidents so that others can learn from them. There are five reasons why you should do so:

1. The first reason is moral. If we have information that might prevent an accident, then we have a duty to pass on that information to those concerned.
2. The second reason is pragmatic. If we tell other people about our accidents, then in return they may tell us about theirs, and we shall be able to prevent them from happening to us. If we learn from others but do not give information in return, we are "information parasites," a term used by biologists to describe those birds, for example, that rely on other species to give warnings of approaching enemies.
3. The third reason is economic. Many companies spend more on safety measures than some of their competitors and thus pay a sort of self-imposed tax. If we tell our competitors about the action we took after an accident, they may spend as much as we have done on preventing that accident from happening again.

4. The fourth reason is that if one company has a serious accident, the whole industry suffers in loss of public esteem, while new legislation may affect the whole industry. So far as the public and politicians are concerned, we are one. To misquote the well-known words of the poet, John Donne:

   > No plant is an Island, entire of itself; every plant is a piece of the Continent, a part of the main. Any plant's loss diminishes us, because we are involved in the Industry: and therefore never send to know for whom the inquiry sitteth; it sitteth for thee.

5. The fifth reason is that nothing else has the same impact as an accident report. If we read an article that tells us to check modifications, we agree and forget. If we read the reports in Chapter 2, we are more likely to remember.

If your employers will not let you publish an accident report under your own name, perhaps they will let you send it to a journal that will publish it anonymously, for example, the *Loss Prevention Bulletin* (see Recommended Reading), or perhaps they will let you publish details of the action you took as a result. This may not have the same impact as the report, but it is a lot better than nothing (see Section 8.1.5).

"IT'S NOT LIKE THAT TODAY"

Some of the accidents in this book occurred during the 1990s. Others go back several decades, a few even earlier. In every walk of life, if we describe something that happened a number of years ago, someone will say, "Schools/hospitals/offices/factories aren't like that any more." Are the old reports still relevant?

In many ways factories, at least, ARE like they used to be. This is not surprising, as human nature is a common factor. We have better equipment but may be just as likely as in the past to cut corners when we design, construct, operate, test, and maintain it, perhaps more likely as there are fewer of us to keep our eyes open as we go round the plant and to follow up unusual observations. We have access to more knowledge than our parents and grandparents, but are we any more thorough and reliable?

We have gotten better at avoiding hazards instead of controlling them, as discussed in Chapter 21, but there is still a long way to go.

Appendix 3

Recommended Reading

Descriptions of other case histories can be found in the following publications.

1. F. P. Lees, *Loss Prevention in the Process Industries,* 2nd edition, Vol. 3, Butterworth-Heinemann, Oxford, UK, 1996.
2. C. H. Vervalin (editor), *Fire Protection Manual for Hydrocarbon Processing Plants,* Vol. 1, 3rd edition, 1985 and Vol. 2, 1981, Gulf Publishing Co., Houston, Texas.
3. *Safety Training Packages,* Institution of Chemical Engineers, Rugby, UK. The notes are supplemented by slides, and some, including one on *Control of Exothermic Chemical Reactions,* are supplemented by videos.
4. *Loss Prevention Bulletin,* Published every two months by the Institution of Chemical Engineers, Rugby, UK.
5. *Safety Digest of Lessons Learned,* Vols. 2–5, American Petroleum Institute, New York, 1979–1981.
6. *Hazard of Water, Hazard of Air, Safe Furnace Firing,* etc., Nine booklets published by The American Oil Company, Chicago.
7. *Case Histories,* Chemical Manufacturers Association, Washington, D.C. No new ones are being published, but bound volumes of old ones are available. They are, however, rather brief.
8. R. E. Sanders, *Management of Change in Chemical Plant—Learning From Case Histories,* Butterworth-Heinemann, Oxford, UK, 1993.

9. *Operating Experience Weekly Summary,* published by the Office of Nuclear and Safety Facility, U.S. Dept. of Energy, Washington, D.C. The incidents described occurred in nuclear facilities, but many contain lessons of wider interest.

Reports about safety originally published by Her Majesty's Stationery Office are now supplied by HSE Books, Sudbury, UK.

Index

Abbeystead, 73
Absorbents, 311
Absorption, 60, 72–73, 374
Access, 52, 82, 150–151, 166, 190, 256
Acetone, 233, 291–292, 330
Acetylene, 375
Acids, 19, 22, 25, 133, 153, 193, 241, 268, 300, 304, 333, 383, 388–389 (*see also* Sulfuric acid)
Acrolein, 385–386
Aerosols, 70–71
Air coolers, 13, 208
Air masks, 26, 55, 106, 230–231, 238–240, 249–250, 253, 256
Aircraft, 100, 104, 302, 361
Alarms, 19, 67, 82, 86-93, 108-109, 130, 139, 177, 227, 245, 247, 254, 269, 272, 276, 278, 283, 330, 359
Alcohol, 62
Alertness, 199, 241, 270, 317, 362 (*see also* Attention, lapses of)
Aluminum, 206, 300, 305, 386
Ambiguity, 14–15
Ammonia, 40, 62, 66, 71, 116, 158, 192, 195–196, 328, 332–333, 340, 343–345, 385
Ammonium nitrate, 333
Analog vs. digital readings, 102
Analysis, 241, 254, 269, 279, 301, 316 (*see also* Combustible gas detectors)
Aqua regia, 388
Arrestors (*see* Flame arrestors)
Asbestos, 104
Assembly, incorrect, 79–80, 186, 378
Attention, lapses of, 78–86, 200–201, 226, 234, 310 (*see also* Alertness)
Attenuation, 375
Autoclaves, 11
Auxiliary materials, reaction with, 387

Backflow (*see* Reverse flow)
Ball check cocks, 148
BCFs, 71
Bearings, 231
Bellows, 56–57, 80, 149, 186–188
Benzene, 18, 140, 145, 158, 217, 306, 378
Bhopal, 368–372
"Black boxes," 354–360
Blame, 79–80, 89
Bleaching powder, 380
BLEVEs, 165–171
Blind eyes, 26–27, 44
Blinds (*see* Maintenance, isolation for)
Boilers, 56, 215–216, 227, 235–236, 312
Boiling liquid expanding vapor explosions (BLEVEs), 165–171
Boilovers, 129, 216
Botching, 35, 41–42, 93
Branches, small, 176
Brazil, 168–169, 194–195, 343
Breathing air, 30, 55 (*see also* Compressed air)
Breathing apparatus (*see* Air masks)
Brine, 61

Brittle failure, 131, 171, 172, 176, 191, 197, 219, 254, 306, 340, 346
Bromine, 61
Bromochlorofluorocarbons (BCFs), 71
Buckets, 147, 291
Buildings, 69–70, 73, 138, 148, 169, 218, 257, 318, 339
Butadiene, 332, 386
Butane, 10, 71, 99, 113–114, 196
Butylene, 193

Cables, accidental cutting of, 30–31
Canned pumps, 39
Carbon beds, 60, 72–73
"Carbon copy," 59
Carbon dioxide, 71, 105, 113–114, 197–198, 234, 241, 340, 348, 374
Carbon dioxide fire extinguishers, 293
Carbon monoxide, 18, 98, 138
Cars (*see* Motor vehicles)
Catalytic crackers, 18
Catchpots, 55, 104, 217
Caustic soda, 64, 105, 133, 241, 300, 382
Centrifuges, 199, 205–206
Champagne, 386–387
Changes (*see* Modification)
Charcoal filters, 60
Checking, 15, 88, 93, 95, 179, 192, 282, 317 (*see also* Inspections)
Chemicals, labeling of, 104–106
Chimney effects, 323–325
Chlorine, 14, 71–72, 104, 158, 202, 286, 299, 332, 382
Chlorofluorocarbons (CFCs), 70–71, 305
Chokes, 22–23, 41, 43, 52, 59, 65, 90, 99, 112, 116, 118, 125, 140–141, 152. 183, 227, 250, 277, 288, 313, 350
  clearing, 311–313
Circuit breakers, 100–101
Cleaning (*see* Maintenance, removal of hazards before; Tanks)
Clothing, 296, 297 (*see also* Protective clothing)
Coatings, 305 (*see also* Paint)
Cocks, 145
"Coffee grounds," 259
Combined cycle gas turbines, 70
Combined heat and power, 70
Combustible gas detectors, 15–21, 62, 120, 159, 160–162, 168, 170–171, 173, 222–224, 256
Communication, 315–318, 361–362
Complexity, 355–356
Compressed air, 30, 41, 51–52, 55, 94, 106, 112, 193, 200, 244–246, 249–250, 266, 304, 311, 319, 330, 333, 386
Compressor houses, 69–70
Compressors, 14, 26, 40, 56, 79, 98, 138, 183, 245, 278, 259, 303
Computer control, 282, 322, 353–364
  data errors, 360–361
  foreseeable failures, 357
  hardware faults, 353–354, 361
  hazop of, 353–357, 362
  interference with, 362–363
  information provided, 364–365
  modifications, 361–362
  old software, 361–362
  operator interface, 358–359
  overconfidence in, 360
  permits-to-work, preparation of, 363–364
  records, retention of, 360
  software faults, 282, 332, 354–358, 361
  trends, 358
  viruses, 363
Condensers, direct contact, 62
Confined spaces (*see* Entry)
  definition, 241
Conservation vents (*see* Valves, pressure/vacuum)
Construction, 15, 28–30, 120, 179, 182, 193, 196–197, 199–200, 241, 250–253
Containers, open, 147, 291, 338
Containers, sample, 147
Contamination, 73, 363, 385–387
Contractors, 12, 15–17, 23–24, 28, 64, 94, 106, 112, 119–120, 132, 147, 199–200, 233, 236–237, 252, 287
Controls, labeling of, 98–99
Cooling coils, 153–154
Cooling towers, 62, 104–105, 218, 221
Cooling water (*see* Water, cooling)
Copper, 305–306

Corrosion, 21, 56, 62, 110, 115, 130, 143, 172, 180, 186, 192–194, 213, 221, 231, 234, 303–308, 311 (*see also* Rust)
  of procedures, 370
Costs, 303, 367, 373
Couplings, pipe, 80
Crack propagation (*see* Brittle failure)
Cranes, 33
Creep, 191, 225
Crude oil, 126–129
Cryogenic storage, 58, 113, 130, 171–172, 254, 268–269, 375
Crystallizers, 13
Cyclohexane, 56–57, 61, 102, 140
Cylinders, 94, 106, 201–202, 233, 250, 269–270, 286, 344, 389

Dangerous working conditions, 32
Dead-ends, 180–183, 245, 248, 259
Decomposition, 160, 182, 259–260, 270
Demolition, 106
Deposits (in vessels), 229–230, 387–388
Detergents, 63, 386–387
Deviations, 335–338 (*see also* Hazard and operability studies)
Diagnosis of faults, 96, 320–321, 350
Diesel engines, 34, 62, 346–347
Diesel oil, 62, 131, 269
Digital vs. analog readings, 102
Dikes, 89, 127–128, 130, 172, 277
Dioxin, 217, 376
Disasters, public response to, 371–372
Distillation columns, 90, 154, 187, 248, 293, 316, 323, 339, 350, 386
Drain points (*see* Valves, drain)
Drains, 20, 28, 63, 183, 238–239, 333 (*see also* Sewers)
Driers, 5, 245
Drums, 18, 73, 208, 292–293, 310–311, 339
Dusts and powders, 54, 101, 236, 246, 294–296, 307, 319, 337–338, 349
Dye-penetrant tests, 232

Electrical equipment
  flameproof, 41
  isolation of, 10
Electricity, static (*see* Static electricity)
Emergencies, handling, 371–372
Emergency power supplies, 62, 274, 277, 282, 339
Emulsion breaking, 322–323, 374–375
Entry, 11, 23, 55, 189, 229–242, 251–253, 364
  irrespirable atmospheres, 230, 238–239, 251–252
Environment, 69–73 (*see also* Pollution)
Equipment
  design, ignorance of, 35–40
  fragile, 110–117
  leased, 276
  reuse of old, 191, 198–199
  sent outside the plant, 22–24
Erosion, 62
Ethanol, 18
Ethers, 388
Ethyl chloride, 172–174
Ethylene, 5, 58, 90, 146, 216
Ethylene oxide, 87–89, 96, 141, 160, 165, 182, 284, 332, 385, 389
Evaporative cooling, 197, 218–219
Excavations, 29, 31
Expansion, 183–185, 187, 302–303, 311
Expansion joints (*see* Bellows)
Expertise, need for, 57
Explosion venting, 332
Explosions, 2–7, 10, 16–19, 21, 38, 54, 56–57, 64, 69–73, 86–89, 92, 117, 128, 133–140, 144–147, 149, 154, 157, 160, 171, 179, 182, 193–195, 205–207, 210, 215–218, 222–227, 232–237, 242, 245–248, 255–256, 265–266, 269, 277, 290–296, 303, 313, 319–320, 323–324, 332–333, 338, 343–348, 360, 370, 381–388

Fastenings, quick-release, 266–267, 309–311, 357
Fatigue (in metals), 110, 129, 176, 180, 183, 196
Faults (diagnosis of), 96, 320–321, 350
Feyzin, 166–168
Films, thin, of liquid, 246
Filters, 60, 234, 245, 310, 356–357
Fin-fan coolers, 208

Fire detectors, 277
Fire fighting, 71, 126–128, 167, 277–278, 293, 320
Fire water, 54
Firemaster, 105
Fires, 1–5, 10, 14, 17–21, 24, 28, 37, 56–57, 62, 66, 71, 94–95, 99, 106, 125–129, 131, 144, 148, 160, 165–174, 179, 182, 186, 191, 194, 208, 218, 221–222, 225–227, 229, 232–237, 245, 248, 254–260, 265–266, 269, 274, 276, 290–292, 295, 300, 313, 318, 320, 333, 343–348, 384, 388
Flakers, 54
Flame arrestors, 72, 95, 114, 118, 139, 141, 276–277, 347
Flameproof electrical equipment, 41
Flanges, 80, 162–172, 183, 194
Flares, 129, 136–142, 210, 314–315, 324, 368, 370
Flashing liquids, 145, 148, 160, 165–177, 194
Flexibility, 180
Flixborough, 56–57, 61, 132
Foam, 158, 216, 256
Foamovers, 182, 246–248, 258, 322–323, 364
Fog (*see* Mists)
Fragile equipment, 110–117
Frequencies of incidents, 392–394
Fuel–gas, 55, 222
Fuel oil, 223–225, 255
Fugitive emissions, 162–163
Furnaces, 52, 55, 62, 66, 72, 81–83, 98, 145, 180, 209, 221–227, 258–259, 282, 301, 357
  lighting of, 221–225
  tube ruptures, 225–227, 260
Fuses, labeling of, 15, 99

Gas, natural (*see* Natural gas)
Gasholder, sucking–in, 314–315
Gaskets, 69, 179, 194, 299–300, 305, 312
Gasoline, 17, 28, 72, 93, 109, 119–120, 126, 147, 159, 185, 195, 256, 264–265, 296–297
Glycerol, 86
Grinders, 193, 254, 319
Grounding, 266, 277, 290–297

Halon, 71, 278
Hazard and operability studies (hazops), 18, 58, 74, 327–341, 369
  of batch plants, 338–339
  of tank trucks, 340–341
  pitfalls in, 337–338
Heat exchangers, 21, 23–24, 62, 218–221, 258, 321
Heat radiation, 142
Heat transfer oils (*see* Oils, heat transfer)
Heat treatment, 12, 14, 197
Heaters, limiting output of, 375–376
Heavy oils (*see* Oils, heavy)
Helium, 374
Horseplay, 245
Hose connections, 3, 249–250, 254, 266, 268
Hoses, 3, 150–153, 233, 263–266, 294, 378
Hot work (*see* Welding)
Human error, 75–86, 377 (*see also* Attention, lapses of; Slips)
Hydrates, 10, 166
Hydrogen, 7, 60, 111, 122–124, 136, 138, 142, 191, 234, 295, 303–305, 311, 323–324
Hydrogen cyanide, 240, 339
Hydrogen fluoride, 268, 304, 306
Hydrogen peroxide, 318–319
Hydrogen sulfide, 26, 66, 238
Hydrogenation, 60
Hypo (sodium hypochlorite), 104–106

Ice, 140, 180–181, 197, 219
Ignition, 70, 94, 117, 123–129, 138, 145–147, 159–160, 167, 170, 172–173, 205–206, 217–218, 232–233, 257, 290–297, 320, 324, 333, 343–349, 389 (*see also* Static electricity)
  of furnaces, 221–225
Ignorance
  of correct valve positions, 313–314
  of emergency procedures, 384

of equipment design, 35–41, 319
of hazards, 93–94, 165–170, 191, 250–251, 337–338
of material strength, 34–35, 132, 225, 306
of reactions, 381–382
of scientific principles, 94–94, 169
Incinerators, 43
Incompatible chemicals, 64, 319, 320, 369
Inert gases, 249, 256 (*see also* Nitrogen)
Inherently safer design, 354, 367–368
on existing plants, 377
Inhibitors, 116, 386
Injection, water, 158, 186
Inspections, 41, 108, 118, 132–134, 151, 156, 179, 184, 201, 210, 276, 317
Instructions, 14–15, 43, 83–84, 191, 387
Instruments (*see also* Alarms; Interlocks; Trips)
direct measurement, 88–89, 162, 284
labeling of, 101–103
visibility of, 84
Insulation, 8, 52, 69, 129–130, 160, 168, 171, 182, 257, 277, 293, 389
Intensification, 372–373
Interlocking disarmed, 52, 86, 93, 207
Interlocks, 52, 86–89, 93, 96, 207, 226, 235–236, 262–263, 275, 278, 281, 283, 288, 310, 322 (*see also* Trips)
Intermediates, 369
Inventories, 372–373
Isolation
for maintenance (*see* Maintenance, isolation for)
inadvertent, 319

Jet mixing, 216
Jets, 293
Joint breaking, 32–33
Joint ventures, 371
Joints, 69, 80, 175–176, 287
incorrect unbolting of, 34, 40
screwed, 193 (*see also* Plugs)

Keys (for opening valves), 235
Kick-backs, 207, 317
Knock-on effects, 377
Knowledge lost, 182 (*see also* Ignorance)

Labels, 18, 64, 80, 83, 98–105, 250, 277, 317, 319
visibility of, 101
Layering (of liquids), 383–385
Leaks, 16, 21, 28–29, 69–70, 144–163, 179–202, 206, 218–219, 222, 233, 279, 297, 355–357 (*see also* Liquefied flammable gas; Liquefied petroleum gas)
control of, 154–159
detection of, 160–162
encasing of, 35
onto insulation, 160–162
onto water, 28–29, 146, 159–160
sources of, 145–154
testing, 70
Leased equipment, 276
Legionnaires' disease, 183
Level glasses, 148
Level measurements, 61, 90–92, 109–110, 175, 196, 201
Lifting gear, 101
Lightning, 118, 138, 277
Limitation of effects, 375–376
Liquefied flammable gas (LFG), 145–146, 160–161, 165–177, 194, 264, 266 (*see also* Butane; Butylene; Liquefied petroleum gas; Propane; Propylene; etc.)
Liquefied gas, 130
Liquefied nitrogen, 254
Liquefied petroleum gas, (LPG) 38, 59, 67, 147, 158, 165–172, 176, 196, 232–233, 274, 316, 375 (*see also* Butane; Butylene; Liquefied flammable gas; Propane; etc.)
Liquids, flashing (*see* Flashing liquids)
Locations (of plants), 171, 195
Lubricants, 62, 245, 255–256, 259
Lubrication, 91, 208, 268

Machinery failure, 91
Magnesium chloride, 231

Maintenance
  above water, 28–29
  excessive force, 33–34
  hazardous materials introduced, 231–236
  identification for, 10–16
  isolation for, 1–10, 233–236, 327–328
  modifications during, 55–56
  near plant boundaries, 27–28
  on moving machinery, 32
  procedures not followed, 24–32
  quality of, 32–44, 206, 213–216, 221
  removal of hazards before, 16–24, 229–231
  unauthorized, 236–238
  unnecessary, 320–321
Materials of construction, 132, 149–150, 171–172, 174, 176–177, 191–192, 197–198, 206, 299–307 (*see also* Brittle failure; Creep; Stress corrosion cracking)
Measurements
  direct, 88–89, 192, 284
  ignored, 90–93, 174, 316
  of level (*see* Level measurements)
Mercury, 306
Methane, 7, 73, 139, 311
Methanol, 94, 104, 120, 291
Methyl isocyanate, 368–370
Methylamines, 165
Mexico City, 170–171, 194
Mind–sets, 88, 96, 152, 268
Mining, 317
Mists, 167, 193, 255, 258, 265, 323, 347–349
Misunderstandings, 29–31
Mixers, 236
Mixing, 339, 348–349, 382–385
Modification, 14–15, 48–74, 124–128, 200, 226, 278, 295, 319, 322, 348–349, 361–362, 384–385
  chains, 66–67
  control of, 74
  during maintenance, 55–56
  gradual, 66
  minor, 49–54, 124–128, 183, 278, 319, 322
  organizational, 64–65
  process, 60–63, 200, 226, 384–385
  remote effects of, 60–61
  sanctioned, 58–59
  startup, 48–49, 58
  temporary, 56–57, 125
  to computer systems, 361–362
  to improve the environment, 69–74
  to tools, 63–64
Molecular seals, 141–142
Molecular sieves, 246
Motor vehicles, 66, 283, 302, 320, 346–347
Mounding, 168

Naphtha, 16, 70, 118–119, 193, 348
Natural gas, 31, 64, 70, 180, 306
Nitrate–induced cracking, 61
Nitration, 61, 104, 313, 373, 381–384, 387–388
Nitric acid, 104
Nitric acid plants, 344
Nitro–compounds, 328, 373
Nitrogen, 17, 94, 100, 102, 117–120, 126, 130–131, 136–138, 144, 150, 175, 201–202, 205, 218, 234, 236, 239, 241, 248–255, 268–269, 276, 278, 293, 306, 323, 329, 385
Nitrogen trichloride, 71
Nitroglycerin, 373
Noise, 69–70
Nuclear power, 59, 86, 287, 302
Nutrimaster, 105

Oils (*see also* Gasoline)
  crude, 126–129
  diesel, 62, 131, 269
  heat transfer, 145, 225–226, 255, 257
  heavy, 181–182, 247, 255–260
  lubricating (*see* Lubricants)
Oleum, 152
Open containers, 147, 291, 338
Overfilling, 91–92, 108–110, 202, 257, 262–263, 320, 334–335, 375
Overflow devices, 111, 115
Overheating, 207, 225–227, 375–376 (*see also* Foamovers)
Overload (of people), 28, 359

Overpressuring, 50–52, 57, 80, 94, 101, 110–114, 140, 170, 182, 194–197, 244, 319
Overtightening, 69
Oxidation, 279–280, 313, 344
Oxygen, 86, 100, 131, 137, 139, 230–231, 236, 240–241, 246, 254, 268–269, 284, 340, 386
Ozone, 70–71

Paint, 232, 330
Paper mills, 123–124, 237–238, 288, 292
Paraffin wax, 332
Pastry, 374–375
Penny-pinching, 303
Pentane, 109
Permits-to-work (*see* Maintenance)
Peroxides, 375, 388
Phenol, 147, 330
Pipe
  couplings, 80
  failures, 56, 102, 179–195, 306, 344
  supports, 56–57, 183–185, 212, 313
  two duties, 318–319
  underground, accidental cutting of, 31
Pipeline fires, 256
Piper Alpha oil platform, 5
Plastics, 54, 133–134, 173, 388
Pleasure rides, 92
Plugs, 21, 39, 67, 94, 149, 152–153, 173, 193
Pollution, 63, 67, 72, 131
Polyethylene plant, 2–4
Polymerization, 80, 182, 386
Polymers, 116, 231, 255, 386
Polypropylene, 17
Powder (*see* Dusts and powders)
Power supplies (*see* Emergency power supplies)
Pressure surges (*see* Surge pressure)
Pressure tests, 286–287, 345–346
Pressure, trapped, 22, 149, 309–311
Pressure vessels (*see* Vessels)
  opening by operators, 266–267, 309–311, 357
Propane, 166–168, 171–172, 175, 196
Propylene, 17–19, 130, 157, 169–170, 219
Protective clothing, 22, 25–27
Protective systems, 272–287, 368, 370, 373 (*see also* Alarms; Interlocks; Trips)
Publication, need for, 395–396
Pump seals, 207, 312–313
Pumps, 12–14, 29, 40, 43, 87–89, 92, 109, 110, 115, 129, 149, 152–157, 169–170, 173–174, 176, 206–208, 226, 259, 277, 301, 312, 318, 320, 331, 375
  canned, 39
  dead-heading, 207–208
  hydraulic, 102

Qatar, 171–172
Quick-release fastenings, 266–267, 309–311, 357

Radioactivity, 20, 59, 61, 63, 152, 275, 286
Railway carriage doors, 274
Railways, 66, 152, 274, 283, 317
Reactants, order of adding, 369, 374–375
Reactions (*see* Runaway reactions)
Reactors, 56–57, 84, 86–89, 328, 331–333
Readings ignored, 90–91
Record sheets, 91
Recorders, 82–84, 90
Refrigerants, 343–345
Refrigerated storage, 343–345, 368, 370 (*see also* Cryogenic storage)
Reinforcement pads, 192–193
Relief and blowdown review, 48–49
Relief devices, discharge disposal, 216–219
Relief valves, 15, 49–50, 52, 58, 67, 114, 142, 162, 167, 196–197, 209–218, 259, 272, 276, 368, 370, 381, 386
  changing, 210–212
  faults, 213–216
  location, 209
  pilot-operated, 216

registration, 209–210
tailpipes, 212
testing, 215–216
vacuum, 115, 126–127, 217–218
Rescue (from confined spaces), 234–235, 239–240, 252–254
Responsibilities, need to define, 277, 314–315
Restriction plates, 54, 210
Reverse flow, 327–333 (*see also* Valves, check)
back into plant, 327–329
from drains, 337
from reactors, 331–333
into service lines, 329–330
through pumps, 331
Rodding out, 311–312
Runaway reactions, 61, 80, 86–89, 148, 217, 328, 360, 368, 376
testing for, 381, 387
Rupture discs, 67, 80, 200, 216–217, 346, 380–387
Rust, 115, 120, 182, 185, 202, 230–231, 240, 255, 305, 385

Sabotage, 368–370
Sample containers, 147
Sampling, 99, 176, 241
Scaffolding, 11, 57
Scale-up, 349–350, 382
Scrap, 24, 302
Scrubbing systems, 368, 370
Sealing plates, 211–212
Self-heating, 389
Service lines, 99, 150, 259, 287, 329–330
Seveso, 217, 376
Sewers, 20, 63–64, 112, 160
Shanty towns, 171, 195, 368–369
Shipping, 287–288, 293, 348
Shutdowns, 91, 316
Sight-glasses, 148
Simplicity, 142, 377
Siphons, 115, 125
Slip-plates (*see* Maintenance, isolation for)
Slips (of memory), 78–90
Slope of ground, 59, 145, 167–168
Slopovers (*see* Foamovers)
Slops, 106, 323
Smoke detectors, 277
Soda, caustic (*see* Caustic soda)
Sodium hypochlorite (hypo), 104–106
Software faults, 282, 322, 354–364
Solvents, 8, 71, 73, 147, 206, 232, 255, 257, 374
Sources of problems lie elsewhere, 60, 350
Spades (*see* Maintenance, isolation for)
Spares 56
Spargers, 62
Spark arrestors, 347
Spill absorbents, 110
Splash filling, 123–124, 265, 292, 295
Sprays, 165
Sprinklers, 62
Stacks, 136–141, 314
choked, 58, 140–142
explosions in, 133–140, 324
Stand-by, 91, 316
Startup, 48, 58
Static electricity, 117, 119, 124, 265–266, 290–297, 337–338
from clothing, 196–297
from gas and water jets, 293–294
from liquids, 291–292
from powders and plastics, 194–196, 348
Steam, 16, 18, 21, 35, 58, 66, 81–82, 91, 99, 115, 126, 138–141, 150, 180–181, 184, 188–189, 196, 199, 218, 234–235, 312, 329
Steam curtains, 157–158, 170
Stéam traps, 188–191, 277
Storage (*see* Drums; Tanks)
reduction of, 287, 372
Stress corrosion cracking, 61, 133, 304, 306–307, 312
Submarines, 288
Substitution, 374–375
Sulfuric acid, 31, 64, 104, 133, 303–304, 312
Sumps, 20, 129, 162, 259
Supports
for instruments, 181
for pipes, 56–57, 183–185
Surge pressure, 66, 158, 185, 188–191, 219–221, 258

Switch filling, 265
Symptoms, treating (instead of causes), 40–41, 220

Tank cars and trucks, 59, 67, 94, 99–100, 115, 124, 152, 262–270, 300, 304, 340–341, 344, 355
  cleaning, 349
  connected to wrong equipment, 268–270
  contact with power lines, 270
  damage to hoses, 263–266
  emptying, 266–270
  fires and explosions in, 265–266, 277, 349
  overfilling of, 262–263
  tipping up, 267–268
Tanks, 7, 11, 16–19, 52, 58, 72, 90–95, 108–134, 141, 377
  acid, 19
  blanketing of, 117–118, 130–131
  break, 332
  entry (*see* Entry)
  fires and explosions in, 18, 117–129, 131, 255, 303, 343, 345
  floating-roof, 117, 125–129, 337
  foamovers in, 246–248
  foundations, 130
  FRP, 111, 133–134
  in ships, 293
  overfilling, 91–92, 108–110
  overpressuring, 110–114, 120
  plastic, 111, 133–134, 248
  rupture of, 110–111, 345
  sucking in, 95, 114–117, 129
  underground, 129
  vents, 7, 95, 110–111, 114–117
Tapping, hot, 54
Teamworking, 317–318
Temperature cycling, 220–221
Tests, 30–31, 82–83, 93, 119–120, 151–153, 157, 195–196, 200–201, 215–216, 272–278, 345–346 (*see also* Combustible gas detectors)
  like real life, 272–275
  ultrasonic, 287
Thermocouples, 40
Three Mile Island, 96–97
Titanium, 24, 299, 307, 333
TNT, 384
Toluene, 318
Tools, 63–64
  accounting for, 42
Toxicity, 6, 26, 105, 230–233, 238–240, 242, 306, 318, 328, 369, 375 (*see also* Ammonia; Chlorine; etc.)
Trace heating, 140, 276–277
Training, 41, 43, 74, 78, 90–97, 116–117, 371, 387–388 (*see also* Ignorance)
Trapped pressure (*see* Pressure, trapped)
Trichlorethylene, 232
Trips, 82–83, 109, 177, 207, 216, 245, 262, 272–274, 276–283, 332, 370
  disarming of, 281–283, 370
  resetting, 281
  response time, 273–274
Two-phase flow, 370

U-bends, 248, 311–312, 333
Ultrasonic testing, 287
Units confused, 102
Uranium hexafluoride, 202
Use-by dates, 388–389
User-friendly design, 377–378

Vacuum, 62, 65, 80, 95, 196, 199, 314, 339, 350 (*see also* Tanks, sucking in; Vessels, sucking in)
Valves
  actuators for, 35–38
  blowdown, 95
  check, 52, 99, 149, 154–157, 207, 210, 264, 274–275, 331
  compressor, 79
  control, 54, 273
  depressuring, 168
  drain,21, 33, 38, 54, 92, 108, 125, 145–146, 166–167, 170, 174, 235–236, 281, 288, 312, 323–324, 337
  emergency isolation, 40, 146, 154–159, 167, 173, 207, 264, 266, 276, 300, 340
  excess flow, 67, 266, 276
  interlocked, 52

let-down, 52
pressure/vacuum, 115, 126
relief (*see* Relief valves)
remotely operated, 92
set incorrectly, 313–314
spring-loaded, 146
Vent collection systems, 72–73
Ventilation, 20, 54, 69–70, 147, 169, 232–233, 242, 249, 277, 318, 345
Venting (of explosions), 295
Vents, 7, 20, 52, 58, 72–73, 90, 95, 110–111, 114–117, 138–141, 146–148, 210, 259, 267, 276–277, 304, 316, 324
Vessels (*see also* Tanks)
entry (*see* Entry)
failure, 124–125, 195–202, 254 (*see also* BLEVEs; Runaway reactions)
glass-lined, 304
multiwall, 195
sucking in, 196, 199
Vibration, 54, 100, 183
Vinyl chloride, 12, 37, 165, 333
Viruses (computer), 363
Warnings ignored, 86–93
Water, 123–124, 246–248, 307
cooling, 57, 61–62, 73, 153–154, 219, 307, 315, 328–333, 385–386
draining, 145, 166–169, 174, 258
hammer (*see* Surge pressure)
heaters, 248
hot, 33, 133, 248
injection, 158, 186
jets, 230
maintenance above, 28
seals, 139–140
sprays, 159, 168, 171
town, 330
Weighing, 202,
Welding, 14–21, 28, 41, 95, 120, 132–134, 149, 199, 232, 246, 256, 301, 307, 333, 343
Wicks, 257

Xylene, 104, 230

Zinc, 122–123
Zoalene, 381

Trevor Kletz, D.Sc., F.Eng., a process safety consultant, has published more than a hundred papers and nine books on loss prevention and process safety, including most recently *Lessons From Disaster: How Organizations Have No Memory and Accidents Recur* and *Computer Control and Human Error.* His experience includes thirty-eight years with Imperial Chemical Industries Ltd., where he served as a production manager and safety adviser in the petrochemical division, and membership in the department of chemical engineering at Loughborough University, Leicestershire, England. He is currently senior visiting research fellow at Loughborough University.

Cover design by Daniell Christian McCleney.
Cover photo courtesy of Gulf Publishing Company Video Training Division.

G|P P
Gulf Professional Publishing
an imprint of Elsevier Science

FOURTH EDITION

WHAT WENT WRONG?

Case Histories of Process Plant Disasters

Praise for previous editions

"It's all here—critical information, advice, and facts—and no professional engineer concerned with designing, operating, or maintaining process plants should be without a copy!"

—*Health and Safety at Work*

". . . easy reading. I highly recommend this book to process design, safety/loss prevention, and operating (production) engineers who will find it useful as a 'checklist' during the process design or hazard analysis stage of a project."

—*Chemical Engineering Progress*

"There are important lessons to be learned in this book, which is directed at a far wider audience than the chemical industry. . . . thought-provoking work . . ."

—*Chemistry and Industry*

"The case histories provide insight into what went wrong, why it went wrong, and how to avoid similar catastrophes."

—*Industrial Safety and Hygiene News*

Visit Gulf at www.bh.com/gulf

PRODUCT #5920

ISBN 0-88415-920-5

50000

9 780884 159209